CISCO SYSTEMS
__||||__..__||||__®

Cisco Customer Response Applications Administrator Guide

Cisco IPCC Express, Cisco IP IVR, and Cisco IP QM, Version 3.5

Cisco Customer Response Applications Administrator Guide

CONTENTS

P A R T 2   **Cisco Customer Response Applications: Configuration**

C H A P T E R 2   **Configuring Cisco CallManager for Cisco CRA** 2-1

C H A P T E R 3   **Setting Up the Cisco IP Telephony Directory** 3-1

CHAPTER 18   **The Tools Menu** 18-1

I N D E X

Preface

The *Cisco Customer Response Applications Administrator Guide* provides instructions for using the Cisco Customer Response Applications (CRA) Administration web interface to provision the subsystems of the Cisco CRA package and to configure Cisco CRA applications.

This guide shows you how to implement three systems that integrate with the Cisco CRA Platform:

- Cisco IP Interactive Voice Response (IVR)

- Cisco IP Integrated Contact Distribution (ICD)

- Cisco IP Queue Manager (IP QM)

This guide also includes a reference section that describes all the menus and menu options of the CRA Administration web interface.

This guide will help you to:

- Perform initial configuration tasks.

- Administer applications, the CRA Engine, and other components of the Cisco IP telephony framework.

- Familiarize yourself with the menus and menu options of the CRA Administration web interface.

Audience

The *Cisco Customer Response Applications Administrator Guide* is written for business analysts and application designers who have the domain-specific knowledge required to create multimedia and telephony customer response applications. Experience or training with Java is not required but is useful for making best use of the capabilities of the Cisco IP telephony framework.

Organization

This guide is divided into three parts. Part 1,
"Cisco Customer Response Applications: Overview", provides an overview of the Cisco Customer Response Applications (CRA) components. Part 2,
"Cisco Customer Response Applications: Configuration," describes the tasks necessary for configuring Cisco CRA. Part 3,
"Cisco Customer Response Applications: Reference," describes the menu options of the CRA Administration web interface and the available real-time reports.

Part 1 contains the following chapters:

Chapter	Title	Description
Chapter 1	Introducing Cisco CRA	Describes key features of the Cisco CRA system. Provides an overview of the configuration tasks necessary to configure and administer Cisco CRA.

Part 2 contains the following chapters:

Chapter	Title	Description
Chapter 2	Configuring Cisco CallManager for Cisco CRA	Describes how to configure Cisco CallManager to communicate with the Cisco CRA server.
Chapter 3	Setting Up the Cisco IP Telephony Directory	Describes the steps required to configure your Cisco IP telephony directory server.
Chapter 4	Provisioning Telephony and Media	Introduces the CRA telephony and media subsystems and describes how to provision subsystem resources and configure subsystem settings.
Chapter 5	Provisioning Cisco IP ICD	Describes how to provision Cisco CallManager and the Cisco IP ICD subsystem.
Chapter 6	Provisioning Additional Subsystems	Describes how to provision the Cisco CRA ICM (Intelligent Contact Management), HTTP, Database, and eMail subsystems.
Chapter 7	Configuring Cisco Script Applications	Describes how to configure Cisco script applications.
Chapter 8	Configuring Additional CRA Applications	Describes how to configure Cisco Busy applications, Cisco Ring-No-Answer applications, Cisco ICM post-routing applications, and Cisco ICM translation-routing applications.
Chapter 9	Managing the Cisco CRA Historical Report Databases	Describes how to configure the database server, schedule data synchronization, configure historical report users, and set up automatic and manual purging of the Cisco CRA historical reports databases.

Chapter	Title	Description
Chapter 10	Managing the Cisco CRA Engine	Describes how to start and stop the CRA Engine and access tracing configuration and log files.
Chapter 11	Reporting on Real-time CRA Data	Describes how to run real-real reports on CRA data. Provides directions for launching sub-reports, printing reports, refreshing reports, and setting report options.
Chapter 12	Updating the JTAPI Client	Describes how to update the JTAPI Client on the Cisco CRA and Cisco Agent Desktop if you install a different version of Cisco CallManager after configuring the CRA system.

Part 3 contains the following chapters:

Chapter	Title	Description
Chapter 13	Overview of the CRA Administration Web Interface	Provides an overview of the CRA Administration web interface.
Chapter 14	The System Menu	Describes the options under the System menu of the CRA Administration menu bar.
Chapter 15	The Applications Menu	Describes the options under the Applications menu of the CRA Administration menu bar.
Chapter 16	The Scripts Menu	Describes the options under the Scripts menu of the CRA Administration menu bar.
Chapter 17	The Subsystems Menu	Describes the options under the Subsystems menu of the CRA Administration menu bar.

Chapter	Title	Description
Chapter 18	The Tools Menu	Describes the options under the Tools menu of the CRA Administration menu bar.
Chapter 19	The Help Menu	Describes the options under the Help menu of the CRA Administration menu bar.

Related Documentation

Refer to the following documents for further information about Cisco CRA applications and products:

- *Cisco Customer Response Applications Getting Started Guide*
- *Cisco Customer Response Applications Serviceability Guide*
- *Cisco Customer Response Applications Historical Reports User Guide*
- *Cisco Customer Response Applications Developer Guide*
- *Cisco Customer Response Applications Editor Step Reference Guide*
- *Cisco Customer Response Applications Troubleshooting Guide*
- *Getting Started with Cisco Customer Response Applications*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords appear in **boldface** font.
italic font	Arguments for which you supply values appear in *italic* font.
[ ]	Optional elements appear in square brackets.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	Nonquoted sets of characters (strings) appear in regular font. Do not use quotation marks around a string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays appear in `screen` font.
`boldface screen` font	Information you must enter appears in **`boldface screen`** font.
^	The key labeled Control is represented in screen displays by the symbol ^. For example, the screen instruction to hold down the Control key while you press the D key appears as ^D.
< >	Nonprinting characters, such as passwords, appear in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in this guide.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the following are useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

CISCO SYSTEMS

P A R T 1

**Cisco Customer Response
Applications: Overview**

Introducing Cisco CRA

The Cisco Customer Response Applications (CRA) platform provides a multimedia (voice, data, and web) IP-enabled customer-care application environment that enhances the efficiency of contact centers by simplifying business integration, easing agent administration, increasing agent flexibility, and enhancing network hosting.

This chapter explains key components of Cisco CRA, describes the CRA product family, and provides an overview of the configuration tasks that will be explained in detail in subsequent chapters.

After you have configured Cisco CRA, you may perform administration tasks such as managing the CRA Engine, running real-time reports, and updating the JTAPI Client (if you change the Cisco CallManager version being used with the CRA system).

This chapter includes the following sections:

Cisco IP Telephony Components

Figure 1-1 shows the components of the Cisco IP Telephony solution.

Figure 1-1   Cisco IP Telephony Solution Components
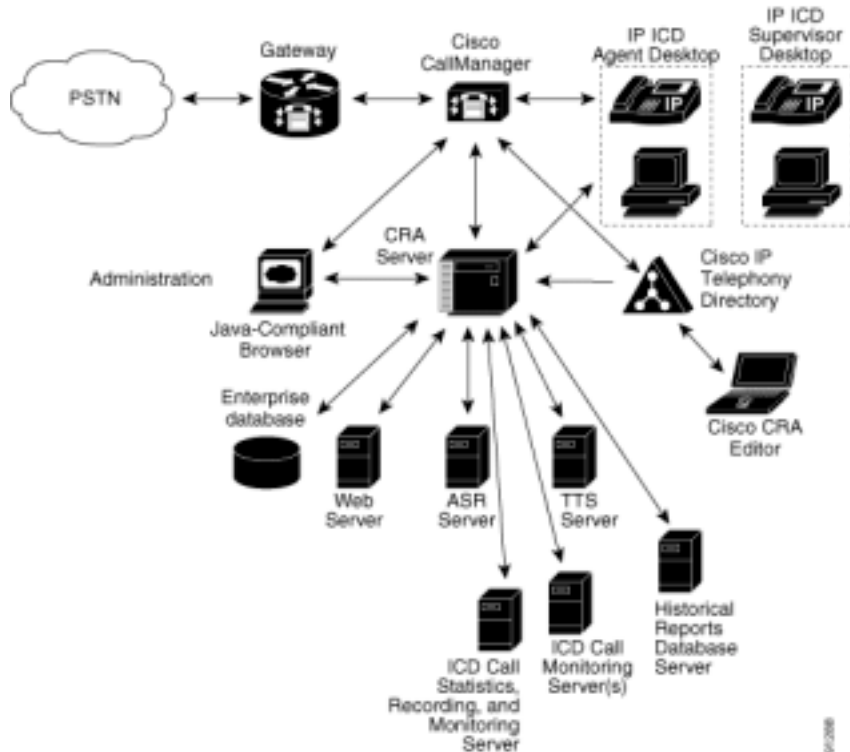
A Cisco IP telephony solution system contains the following components:

- Gateway—Connects the enterprise IP telephony network to the Public Switched Telephone Network (PSTN) and to other private telephone systems such as PBX.

- Cisco CallManager server—Provides the features required to implement IP phones, manage gateways, provide failover and redundancy service for the telephony system, and direct Voice over IP (VoIP) traffic to the Cisco CRA system.

- Cisco IP Telephony Directory—Stores configuration information, applications, and Cisco scripts in a Lightweight Directory Access Protocol (LDAP) directory. Storing applications and scripts in an LDAP directory allows you to share all Cisco CRA applications and scripts on all Cisco CRA servers in the network. The Repository keeps one backup version of each script for recovery purposes.

- CRA application server—Contains the CRA Engine that runs applications., including Cisco script applications, Cisco Intelligent Contact Manager (ICM) translation-routing and post-routing applications, Busy applications, and Ring No Answer (RNA) applications. You can position your Cisco CRA application server anywhere on the IP network and administer your applications from a web browser on any computer on the IP network. Because Cisco CRA uses an open architecture that supports industry standards, you can integrate your applications with a wide variety of technologies and products such as Enterprise databases and Cisco IP ICD (Integrated Contact Distribution) Agent Desktop.

- Cisco CRA Editor—Allows application developers to use a simple graphical user interface (GUI) to create, modify, and debug Cisco CRA scripts for automating customer interactions. Each script consists of a series of steps, implemented as Java Beans.

- Cisco CRA Administration web interface—Allows administrators to use a web browser to configure and manage Cisco CRA applications.

- Cisco IP Agent and Supervisor Desktops —Desktop programs that allow ICD agents and supervisors to log into the system, change agent states, and monitor status.

- Nuance Automatic Speech Recognition (ASR) server—Dedicated server that performs real-time speech recognition.

- Text-to-Speech (TTS) server—Dedicated server that converts text into speech and plays it back to the caller.

- ICD Call Statistics, Recording, and Monitoring server—Dedicated server that maintains ICD call statistics and that provides for recording and call monitoring for Cisco ICD Enhanced.

- ICD Call Monitoring servers—Additional dedicated servers that provide for call monitoring.

- Historical Reports Database server—Dedicated server that stores Cisco CRA databases for historical reporting.

The Cisco CRA Product Family

The Cisco CRA product family provides a variety of contact-processing functions for your Cisco IP Telephony solution.

The software package you choose determines which steps, components, and subsystems you receive. (Each CRA product includes the CRA Engine and the CRA Editor.)

The Cisco CRA product family includes the following packages:

- Cisco IP IVR, page 1-4
- Cisco IP ICD, page 1-5
- Cisco IP Queue Manager, page 1-6

Cisco IP IVR

Cisco IP Interactive Voice Response (IVR) is a multimedia (voice, data, web) IP-enabled interactive voice response solution that offers an open and feature-rich foundation for the creation and delivery of IVR applications via Internet technology.

Cisco IP IVR automates call handling by autonomously interacting with contacts. Using Cisco IP IVR, you can create applications that answer calls, provide menu choices for callers, obtain caller data such as passwords or account identification, and transfer calls to caller-selected extensions. You can also create IP IVR applications that respond to HTTP requests and send e-mail.

The Cisco IP IVR package provides the following features:

- Cisco IP Contact Center (IPCC) integration—IP IVR can be integrated with IP Queue Manager (IP QM) functionality to participate in the Cisco IPCC solution.
- Open Database Connectivity (ODBC) support—IP IVR applications can access Microsoft Structured Query Language (SQL) servers and Oracle, Sybase, and IBM DB2 databases.
- Real-time reporting client—IP IVR applications can generate a variety of reports that provide detailed information about the real-time status of your system.

- Historical reporting client—IP IVR applications can generate a variety of historical reports that provide detailed information about the performance of your system.

- Automatic Speech Recognition (ASR)—IP IVR applications can take advantage of ASR to provide callers with the option to use speech to navigate through menu options.

- Text-to-Speech (TTS)—IP IVR applications can use TTS to read back documents and pre-scripted prompts to callers.

Cisco IP ICD

Cisco IP Integrated Contact Distribution (ICD) is an IP-based automated call distribution (ACD) system that queues and distributes incoming calls destined for groups of Cisco CallManager users.

You can use Cisco IP ICD applications to route calls to specific agents. You can also integrate Cisco IP ICD with Cisco IP IVR to gather caller data and classify incoming calls.

Cisco IP ICD includes a web-based real-time and historical reporting system that you can use to monitor system, Contact Service Queue (CSQ), and resource performance.

The Cisco IP ICD system consists of the following major components:

- Resource Manager—Application program that monitors ICD agent phones and allows you to organize agents into resource groups or skills-based partitions according to the types of calls each group can handle.

- Contact Service Queue (CSQ)—Application program that places incoming calls in a queue and distributes them to the appropriate set of agents as the agents become available.

- ICD Agent Desktop—Application program that ICD agents run on their desktop computers to log in to the system, change ICD state, and monitor status.

The following licensing options are available for the Cisco IP ICD system:

- IP ICD Standard (designed for entry-level users)—Includes the steps necessary for creating basic ICD applications.

- IP ICD Enhanced (designed for enterprise-level users)—Includes all functions of IP ICD Standard, plus steps that allow for assigning call priority.

- IP ICD Enhanced with CTI (Computer Telephony Interface) Option (available only to ICD Enhanced customers)—Adds full IP IVR support, except for ICM (Intelligent Contact Management) integration, including database integration, Voice eXtensible Markup Language (VoiceXML), HTML web integration, custom Java extensions, and e-Notification services.

Cisco IP Queue Manager

Cisco IP Queue Manager (IP QM) is an IP-based call treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution, which is a high-end contact center solution capable of distributing calls to multiple sites and performing powerful pre- and post-routing functions.

You can use Cisco IP QM to allow callers to select routing options, and to provide callers with easy access to multiple agent skill groups, extensions, or announcements, either before or after routing.

Cisco IP QM call-treatment messages can be static, prerecorded announcements or dynamic announcements tailored to specific caller interests. Cisco IP QM can provide dynamic content to queued callers, delivering unique messages tailored to each caller's needs, the route selected, the caller's place in the queue, or other associated values.

Cisco IPCC uses Cisco Intelligent Contact Manager (Cisco ICM) software to direct calls to other systems such as interactive voice response units (VRUs) and ACD (Automated Call Distribution) systems.

You use the ICM VRU interface included with IP QM to configure the CRA server to work with Cisco IPCC. Cisco ICM scripts can use the ICM VRU interface to invoke Cisco CRA Editor steps and logic from the CRA Engine to handle calls centrally and direct them to your IP Telephony system based on caller- entered data, information stored in a database, or other parameters.

Note   Only customers who use both Cisco IPCC and Cisco ICM can use the ICM VRU
interface.

About the Cisco CRA Engine

The Cisco CRA Engine enables you to run multiple applications to handle Java
Telephony Application Programming Interface (JTAPI) calls or HTTP requests.

While you can deploy the Cisco CRA Engine and Cisco CallManager on the same
server, deploying them on separate servers allows you to handle greater call
volume.

The CRA Engine uses JTAPI to request and receive services from the Computer
Telephony Interface (CTI) manager that controls Cisco CallManager clusters. The
Cisco CRA Engine is implemented as a Windows service that supports multiple
applications.

You can use a web browser to administer the CRA Engine and your CRA
applications from any computer on the network. You can use the
CRA Administration web interface to start and stop the CRA Engine, configure
system parameters, monitor CRA Engine activity, and view real-time and
historical reports that include total system activity and application statistics.

Depending on the Cisco CRA products that you are using, the CRA server may
employ as many as 14 subsystems for communicating with other services:

- Applications—Manages the applications in the CRA Engine and other
  features such as session management.

- Cisco Media—Configures Cisco Media Termination (CMT) dialog control
  groups, which can be used to handle simple Dual Tone Multifrequency
  (DTMF) based dialog interactions with customers.

- Core Reporting—Provides information for IP IVR real-time reports.

- Database—Handles the connections between the CRA server and the
  enterprise database.

- eMail—Adds components to the CRA Engine that allows it to send e-mail
  messages.

- Enterprise Server—Communicates data for screen pops to the
  Cisco Agent Desktop.

Cisco Customer Response Applications Administrator Guide

- HTTP—Adds components to the CRA Engine that allow it to respond to HTTP requests.
- ICM (Intelligent Contact Management)—Manages the connection between the CRA server and Cisco Intelligent Contact Management (Cisco ICM).
- JTAPI (Java Telephony Application Programming Interface)—Manages the connection between Cisco CallManager CTI Manager and the CRA Engine.
- Nuance Automatic Speech Recognition (ASR)—Allows a script to respond to voice input in addition to DTMF.
- Nuance Text-To-Speech (TTS)—Composes voice prompts that are generated in real time from text, such as speaking the words in the text of an e-mail message.
- RMCM (Resource Manager-Contact Manager)—Allows Cisco IP ICD to monitor agent phones, control agent states, route and queue calls, and manage the historical reporting feature.
- Voice Browser—Manages Voice Browser functionality.
- VoIP (Voice over Internet Protocol)—Enables remote recording and monitoring.

Configuration Overview for Cisco CRA

Before you can use your Cisco CRA system, you will need to perform the following series of procedures:

1. Use the Cisco CallManager to configure a JTAPI (Java Telephony Application Programming Interface) user for Cisco CRA, to configure CTI ports and CTI route points, and then to associate them with the JTAPI user.

   If you have purchased IP ICD, you also use Cisco CallManager to configure agents for IP ICD.

2. Set up the LDAP directory that will store configuration information.

3. Provision the CRA subsystems so that the CRA system can run multiple applications to handle JTAPI calls or HTTP requests.

4. Configure the CRA applications that will interact with contacts.

5. Configure the CRA Historical Reporting databases.

This section contains the following topics:

Configuring Cisco CallManager for Cisco CRA

Cisco CallManager provides the features required to implement IP phones, manage gateways, and direct Voice over IP (VoIP) traffic to the Cisco CRA system. Cisco CRA communicates with Cisco CallManager by means of a JTAPI user.

You will begin the configuration process by accessing the Cisco CallManager Administration web interface and performing the following tasks:

1. Create a JTAPI user

2. Configure CTI ports

3. Configure CTI route points

4. Associate the CTI ports and CTI route points with the JTAPI user.

5. Configure users in Cisco CallManager if you have purchased an IP ICD package.

See Chapter 2, "Configuring Cisco CallManager for Cisco CRA," for the detailed configuration procedures necessary for accomplishing these tasks.

Setting up the Cisco IP Telephony Directory

After you configure Cisco CallManager for Cisco CRA, you will need to configure directory information.

To continue the CRA system configuration process, you will connect to the Cisco CRA Administration web interface and perform the following tasks:

1. Specify the directory that will be used to store configuration information. You can use the default DC (Data Connection) directory that comes with the CRA system, or you can use either Netscape Directory or Microsoft Active Directory.

2. Choose the profile name that identifies the CRA server repository. The repository is a subdirectory of the LDAP directory (the directory in which the Cisco CRA system stores configuration information). The repository stores applications and Cisco scripts.

3. Configure your configuration and repository profiles. The configuration profile holds the CRA Engine configuration information that is specific to a single CRA server. The repository profile maintains the scripts and the applications you have created and configured.

4. Assign administrative privileges to selected users.

See Chapter 3, "Setting Up the Cisco IP Telephony Directory," for detailed instructions on connecting to the CRA Administration web interface and setting up the directory that will be used by Cisco CRA.

Provisioning the Cisco CRA Subsystems

After you set up the CRA directory, you need to provision your CRA subsystems to enable the CRA Engine to run multiple applications to handle JTAPI calls or HTTP requests.

Note   You need to configure a particular subsystem only if you are using CRA applications that require it.

To continue the CRA system configuration process, you will connect to the Cisco CRA Administration web interface and perform the following tasks:

- Provision the Telephony and Media Subsystems, page 1-11
- Provision the IP ICD Subsystem, page 1-11
- Provision the Additional CRA Subsystems, page 1-12

Provision the Telephony and Media Subsystems

The four Cisco CRA telephony and media subsystems manage telephony and media resources and communicate with supporting telephony and media systems.

To provision the telephony and media subsystems, you will perform the following tasks:

1. Provision the JTAPI subsystem. The JTAPI subsystem controls the telephony resources for the CRA system.

2. Provision the Cisco Media subsystem. The Cisco Media subsystem controls the Cisco Media Termination (CMT) media resources for the CRA system.

3. Provision the Nuance ASR subsystem. The Nuance ASR subsystem controls the Automatic Speech Recognition (ASR) media resources for the CRA system.

4. Provision the Nuance TTS subsystem. The Nuance TTS subsystem controls the Text-To-Speech (TTS) media resources for the CRA system.

See Chapter 4, "Provisioning Telephony and Media," for detailed instructions on provisioning the Cisco CRA telephony subsystems.

Provision the IP ICD Subsystem

The IP ICD subsystem provides resource distribution and queueing to call centers as part of an Automatic Call Distribution (ACD) system. If you have purchased any of the three versions of Cisco IP ICD, you will need to provision the IP ICD subsystem. (Otherwise, proceed to Chapter 6, "Provisioning Additional Subsystems.")

Note   Before provisioning the IP ICD subsystem, you must configure users in Cisco CallManager. See Configure Users in Cisco CallManager, page 2-10

To continue the CRA system configuration process, connect to the Cisco CRA Administration web interface and perform the following tasks:

1. Provision the RM JTAPI provider. The Resource Manager (RM) of the Cisco IP ICD system uses a Cisco CallManager user (called a JTAPI provider) for monitoring agent phones, controlling agent states, and routing and queueing calls.

2. Provision Resource Groups. *Resource groups* are collections of agents that your CSQ uses to handle incoming Cisco IP ICD calls. To use resource group-based CSQs, you must specify a resource group.

3. Provision Skills (for the two ICD Enhanced packages only). *Skills* are customer-definable labels assigned to agents. The two IP ICD Enhanced packages can route incoming calls to agents who have the necessary skill or sets of skill to handle the call.

4. Provision Resources. Agents that answer calls are also called *resources*. After you create a resource group, you must assign agents (resources) to that group. You can also assign agents to skills if you have purchased either of the IP ICD Enhanced packages.

5. Provision CSQs. After you assign an agent to a resource group, or assign skills to an agent (the two ICD Enhanced packages only), you need to configure the agent for the CSQ to which the agent will be assigned.

See Chapter 5, "Provisioning Cisco IP ICD," for detailed instructions on provisioning the IP ICD subsystem.

Provision the Additional CRA Subsystems

The additional CRA subsystems provide ICM, HTTP, Database, and eMail features.

To continue the CRA system configuration process, connect to the Cisco CRA Administration web interface and perform one or more of the following tasks, as needed:

• Provision the ICM subsystem. The ICM subsystem communicates with Cisco Intelligent Contact Management (ICM).

• Provision the HTTP subsystem. The HTTP subsystem enables CRA applications to respond to requests from a variety of web clients.

- Provision the Database subsystem. The Database subsystem enables CRA applications to communicate with enterprise database servers.

- Provision the eMail subsystem. The eMail subsystem enables CRA applications to create and send e-mail.

See Chapter 6, "Provisioning Additional Subsystems," for detailed instructions on provisioning these four subsystems.

Configuring Cisco CRA Applications

After you provision the CRA subsystems, you need to configure CRA applications to interact with contacts and perform a wide variety of functions.

To continue the CRA system configuration process, connect to the Cisco CRA Administration web interface and perform the following tasks:

- Configure Cisco Script Applications, page 1-13
- Configure Additional CRA Applications, page 1-14

Configure Cisco Script Applications

Cisco script applications perform such functions as receiving calls, playing back prompts, receiving caller input, transferring calls, and queueing calls.

The process of configuring Cisco script applications includes uploading CRA scripts and pre-recorded prompts, installing grammars and customized languages, and adding triggers to applications.

Depending on your particular CRA implementation, you may need to perform most or all of the following tasks to configure a Cisco script application:

1. Manage scripts. Cisco script applications are based on scripts that you must upload to the repository and make available to the CRA system.

2. Manage prompts. Many applications make use of pre-recorded prompts, stored as .wav files, which are played back to callers in order to provide information and elicit caller response. You must upload these .wav files to the repository and make them available to the CRA system.

3. Install grammars. The CRA system uses specific grammars to recognize and respond to caller response to prompts. You must store these grammars in a directory to make them available to the CRA system.

4. Install customized CRA languages. Language packs, such as American English, Canadian French, and so on, are installed with Cisco CRA. You install language packs in a directory accessible by the CRA system.

5. Install Java files. In addition to the Java files automatically installed as part of the Cisco CRA installation process, you can install your own custom classes and Java Archive (.jar) files in order to customize the performance of your CRA system.

6. Add a Cisco script application. You can add scripts to be used as the basis for the Cisco script application.

7. Add an application trigger. Triggers are specified signals that invoke application scripts in response to incoming contacts. After adding a new Cisco script application, you need to add a trigger so that this application can respond to telephone calls and/or HTTP requests.

See Chapter 7, "Configuring Cisco Script Applications," for detailed instructions on configuring CRA script applications.

Configure Additional CRA Applications

Other script applications perform such functions as providing busy signals and ringing tones, and to provide ICM post-routing and translation-routing.

To configure these additional CRA applications, you will need to perform the following tasks:

1. Configure the Busy application. This application, which comes with each CRA package, simulates a busy signal.

2. Configure the Ring-No-Answer (RNA) application. This application, which comes with each CRA package, simulates a ring tone.

If you are using Cisco ICM, you will also need to perform one or both of the following tasks:

- Configure ICM post-routing applications. The Cisco IP IVR (Interactive Voice Response) system uses ICM (Intelligent Contact Management) post-routing applications to receive calls directly from Cisco CallManager, which sends the call to the post-routing route point on the Cisco CRA system.

- Configure ICM translation-routing applications. These applications use the CRA server as a queue point for Cisco IPCC (IP Call Center), so that Cisco ICM can route calls to the CRA server.

See Chapter 8, "Configuring Additional CRA Applications," for detailed instructions on provisioning these additional CRA applications.

Configuring Cisco CRA Historical Reporting Databases

When you install the Cisco CRA system, the installation procedure creates two databases that the system uses to store data for historical reports:

- Db_cra—The main CRA database, which contains most information for historical reports, including information about agents, skills, and resources.

- Db_cra_ccdr—The additional CRA database, which contains information about each call that the system processes.

The Cisco CRA system historical databases can reside either on the CRA server machine or on the Historical Reports Database server machine. The Historical Reports Database server is installed on a separate machine from the CRA server; they cannot be co-located.

To conclude the CRA system configuration process, connect to the Cisco CRA Administration web interface and perform the following tasks:

1. Configure the database server if historical reporting data is stored on the Historical Reports Database server.

2. Configure users for historical reports.

3. Make sure the Purging Scheduler Service is running and configure the daily purge schedule and notification parameters.

4. Configure the synchronize data schedule if historical data is stored on the Historical Reports Database server.

See Chapter 9, "Managing the Cisco CRA Historical Report Databases," for detailed instructions on how to configure the CRA historical reporting databases.

PART 2

Cisco Customer Response Applications: Configuration

Configuring Cisco CallManager for Cisco CRA

Cisco CallManager is the software-based call-processing component of the Cisco IP telephony solution that provides the features required to implement IP phones, manage gateways, and direct Voice over IP (VoIP) traffic to the Cisco Customer Response Applications (CRA) system.

The CRA server contains the CRA Engine, which runs applications that interact with contacts. The CRA server communicates with Cisco CallManager by means of CTI (Computer Telephony Interface) ports and route points that are identified by a Java Telephony Application Programming Interface (JTAPI) user number.

This chapter begins the process of implementing your CRA system by showing you how to configure Cisco CallManager to communicate with the CRA server.

Note For information on installing the Cisco CRA operating system and Cisco CallManager, see *Getting Started with Cisco Customer Response Applications*.

To configure Cisco CallManager for use with Cisco CRA, you need to perform the following configuration tasks:

1. Connect to the Cisco CallManager Administration web interface.

   The Cisco CallManager Administration web interface, which is similar to the CRA Administration web interface, allows you to use a web browser to configure Cisco CallManager.

2. Create a JTAPI user.

   The CRA system will use this JTAPI user to communicate with the Cisco CallManager.

3. Add CTI ports.

   The JTAPI subsystem of the CRA system requires one CTI port device for each call it simultaneously places or accepts.

4. Add CTI route points.

   The JTAPI subsystem requires a CTI route point device for each call it simultaneously places or accepts.

5. Associate the JTAPI user with the devices (the CTI ports and route points).

   When the CRA system accesses this JTAPI user, the CRA system makes these CTI ports and CTI route points available.

If your CRA system includes IP ICD, you need to perform these additional configuration tasks:

6. Assign ICD extensions for the users who will be agents in your Cisco IP ICD system.

7. Create a Cisco CallManager user for the Resource Manager (RM) of the ICD subsystem.

Note If you delete a Cisco CRA user from Cisco CallManager, the user will not be able to log into the Cisco CRA Administration web interface.

This chapter includes the following procedures:

Connect to the Cisco CallManager Administration Web Interface

Begin the process of configuring Cisco CallManager by connecting to the Cisco CallManager Administration web interface.

To connect to the Cisco CallManager Administration web interface, complete the following steps.

Procedure

Step 1   Perform one of the following actions:

- From the server running Cisco CallManager, choose **Start > Programs > Cisco CallManager3.2 > CallManager Administration**.
- From a web browser on any computer on your network, enter the following URL: **http://*servername*/ccmAdmin**.

  In this example, *servername* is the host name or IP address of your Cisco CallManager server. The Cisco CallManager Login web page appears.

Step 2   Enter your name and password at the prompt, and then click **Log On**.

The Cisco CallManager 3.2 Administration web page appears.

You are now ready to use the Cisco CallManager Administration web interface to configure JTAPI users, CTI ports, CTI route points, and users for IP ICD (if your CRA system includes IP ICD).

Create a JTAPI User

In order for Cisco CallManager and the Cisco CRA system to communicate, Cisco CallManager must recognize the CRA system as a JTAPI user.

To create a JTAPI user for Cisco CRA, complete the following steps.

Procedure

Step 1   If you have not already done so, connect to the Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

Step 2   From the Cisco CallManager Administration menu bar, choose **User > Add a New User**.

The User Information web page appears.

Step 3   Enter a first name and last name for the Cisco CRA user.

Create meaningful names that are concise, yet easy to recognize, such as "JTAPI User" or "RMUser".

Step 4   In the User ID field, enter a user ID.

Step 5   In the User Password and Confirm Password fields, enter a password.

Step 6   In the PIN and Confirm PIN fields, enter a PIN (Personal Identification Number).

The PIN must contain at least five characters.

Step 7   Check the **Enable CTI Application Use** check box.

If you do not check the **Enable CTI Application Use** check box, the CRA server cannot control or monitor the associated devices.

Step 8   Click **Insert**.

The Application Profile area of the User Information web page is now populated with the user name you entered. Device Association, Extension Mobility, and Softphone hyperlinks also appear.

You are now ready to add CTI ports.

Add CTI Ports

In order to accept or place calls, the JTAPI subsystem requires one CTI port device for each call to be managed simultaneously.

You must configure each device (CTI port) with a single unique directory number. No directory number can be associated with more than one device. No device can be associated with more than one directory number.

Note   Devices that are not properly configured will not be listed as valid devices on the CRA JTAPI configuration web pages.

Directory numbers for Cisco CallManager CTI ports can be non-consecutive. They need not follow a logical structure, although for consistency you may want to use some such schema to assign port numbers.

To add CTI ports in Cisco CallManager for a Cisco CRA application, complete the following steps.

Procedure

Step 1   If you have not already done so, connect to the Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

Step 2   From the Cisco CallManager Administration menu bar, choose **Device > Add a New Device**.

The Add a New Device web page appears.

Step 3   From the Device Type drop-down menu, choose **Phone**, and then click **Next**.

The Add a New Phone web page appears.

Step 4   From the Phone Type drop-down menu, choose **CTI Port**, and then click **Next**.

The Phone Configuration web page appears.

Step 5   In the Device Name field, enter a unique name to identify this device.

Step 6   From the Device Pool drop-down menu, choose the device pool for this CTI port, or if there is no other device pool, choose **Default.**

Step 7   Click the **Insert** button.

A dialog box appears prompting you to add the default directory number for Line 1 of this Phone.

Step 8   Click **OK**.

The dialog box closes, and the Directory Number Configuration web page appears.

Step 9   In the Directory Number field, enter the directory number for this CTI port, and then click **Insert**.

A dialog box appears informing you that the directory number has been assigned to the current device and asking whether you want to return to the current device or stay on the Directory Number page.

Step 10   Click **OK** to return to the current device.

The dialog box closes and the Phone Configuration web page appears

Step 11   To add other CTI ports, repeat Step 2 through Step 10 as needed.

You are now ready to add CTI route points.

Add CTI Route Points

In order to accept or place calls, the JTAPI subsystem requires that each call be assigned a CTI route point device. Because a single route point can handle multiple calls, you do not need a unique route point for each simultaneous call.

You must configure each device (CTI route point) with a single unique directory number. No directory number can be associated with more than one device. No device can be associated with more than one directory number.

Note   Devices that are not properly configured will not be listed as valid devices on the JTAPI configuration web pages.

To add CTI route points in Cisco CallManager for a Cisco CRA application, complete the following steps.

Procedure

Step 1   If you have not already done so, connect to the Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

Step 2   From the Cisco CallManager Administration menu bar, choose **Device > Add a New Device**.

The Add a New Device web page appears.

Step 3   From the Device Type drop-down menu, choose **CTI Route Point**, and then click **Next**.

The CTI Route Point Configuration web page appears.

Step 4   In the Device Name field, enter a name for the CTI route point.

Step 5   From the Device Pool drop-down menu, choose the device pool for this CTI route point, or if there is no other device pool, choose **Default.**

Step 6   Click **Insert**.

A dialog box appears, informing you that the CTI route point has been inserted in the database, and prompting you to add the directory number for Line 1 of this CTI route point now.

Step 7   Click **OK** to add the directory number for Line 1 of this CTI route point.

The dialog box closes, and the Directory Number Configuration web page appears, as shown in.

Step 8   In the Directory Number field, enter the directory number for this CTI route point.

This number is the number that users will dial to reach this CTI route point.

The CRA Engine supports the following characters in the Directory Number of a CTI route point: 0-9, "*", "#", "X", "[", "]", and "-".

For additional information on the use of non-numeric characters, see the section on "Route Pattern Wildcards and Special Characters" in the *Cisco CallManager Administration Guide*.

Step 9   Click **Insert**.

A dialog box appears indicating that the directory number has been assigned to the current device.

Step 10   Click **OK**.

The dialog box closes.

To add other CTI route points, repeat Step 2 through Step 10 as needed

You are now ready to associate devices with the JTAPI user.

Associate Devices with the JTAPI User

Once you have created a JTAPI user, and established CTI ports and CTI route points, you need to associate the devices (CTI ports and route points) with the JTAPI user.

To associate devices with the JTAPI user, complete the following steps.

Procedure

Step 1   If you have not already done so, connect to Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

Step 2   From the Cisco CallManager Administration menu bar, choose **User > Global Directory**.

The User Information web page appears, displaying the Basic Search area.

Step 3   Click **Search**.

The Find and List Users area of the User Information web page appears.

Step 4   Double-click the username you created in the "Create a JTAPI User" section on page 2-4.

The User area of the User Information web page appears.

Step 5   On the User Information navigation bar, click the **Device Association** hyperlink.

The Assign Devices area of the User Information web page appears.

Step 6   In the **Available Device List Filters** area, choose **Directory Number**, choose **Begins With**, and enter the CTI port number you created in the "Add CTI Ports" section on page 2-5.

Step 7   Click **Select Devices**.

The Assign Devices area of the User Information web page refreshes.

Step 8   Scroll down to the **Available Devices** area, and then check the **Type** check box.

Step 9   Click **Update** to apply changes.

The User area of the User Information web page appears.

Step 10   On the User Information navigation bar, click the **Device Association** hyperlink.

The Assign Devices area of the User Information web page appears.

Step 11   In the **Available Device List Filters** area, choose **Directory Number**, choose **Begins With**, and enter the CTI route point number you created in the "Add CTI Route Points" section on page 2-6.

Step 12   Click **Select Devices**.

The Assign Devices area of the User Information web page refreshes.

Step 13   Scroll down to the Available Devices area, and then click the **Type** check box.

Step 14   Click **Update** to associate these CTI ports and CTI route points with the JTAPI user.

The User Information web page appears, with the JTAPI user configuration information displayed.

You are now ready to configure directory information for the CRA server.

(See Chapter 3, "Setting Up the Cisco IP Telephony Directory.")

Configure Users in Cisco CallManager

To use any version of Cisco IP ICD, you must first configure the following two Cisco CallManager parameters for Cisco IP ICD:

- Assign ICD extensions for the users who will be agents in your Cisco IP ICD subsystem.

- Create a Cisco CallManager user for the Resource Manager (RM) of the Cisco IP ICD subsystem.

Note   In Cisco CallManager, these operations are called "assigning a device."

This section contains the following procedures:

Assigning ICD Extensions to Agents

Agent information on the Cisco CallManager is updated in IP ICD at 10-minute intervals. If you modify an agent's record in Cisco CallManager (for example, changing the ICD extension or deleting the agent), the agent's information in the ICD subsystem is updated at the next interval. You can update the IP ICD information in the CRA Administration at any time by selecting Subsystems > ICD and clicking the Resources hyperlink. Also, if you change an agent's ICD extension, the agent must log off and then log back in to the Cisco Agent Desktop to get the new extension.

To configure users to become Cisco IP ICD agents, complete the following steps.

Procedure

Step 1   Connect to the Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

The Cisco CallManager Administration web page appears.

Step 2   From the Cisco CallManager Administration menu bar, choose **User > Add a New User**.

The Add a New User area of the User Information web page appears

Step 3   Click the **Back to User List** hyperlink in the upper right corner.

The Find and List Users area of the User Information web page appears.

Step 4   Under the Last Name column heading, click the user for which you want to enable the ICD extension.

The User Information web page appears and displays this user's information.

Step 5   On the User Information navigation bar, click the **Device Association** hyperlink.

Step 6   The Assign Devices area of the User Information web page appears.

Step 7   In the Available Devices column, check the box next to the device you want to assign to this user.

Make sure the **ICD Ext.** radio button is selected for the device.

Step 8   Click **Update** to apply the changes.

The specific User Information page for this user appears, with the message that the update was successful.

Creating a RM User

If you are using IP ICD, you must create a RM user, which enables communication between the Cisco CallManager and IP ICD.

To create a RM user, complete the following steps.

■ Configure Users in Cisco CallManager

Procedure

Step 1   If you have not already done so, connect to the Cisco CallManager Administration web interface.

For information about connecting to the Cisco CallManager Administration web interface, see Connect to the Cisco CallManager Administration Web Interface, page 2-3.

Step 2   From the Cisco CallManager Administration menu bar, choose **User > Add a New User**.

The User Information web page appears.

Step 3   Enter a first name and last name for the Cisco CRA user.

Create meaningful names that are concise, yet easy to recognize, such as "RMUser".

Step 4   In the User ID field, enter a user ID.

Step 5   In the User Password and Confirm Password fields, enter a password.

Step 6   In the PIN and Confirm PIN fields, enter a PIN (Personal Identification Number).

The PIN must contain at least five characters.

Step 7   Check the **Enable CTI Application Use** check box.

If you do not check the **Enable CTI Application Use** check box, the CRA server cannot control or monitor the associated devices.

Step 8   On the User Information navigation bar, click the **Device Association** hyperlink.

The Assign Devices area of the User Information web page appears.

Step 9   In the Available Devices column, check the box next to the each device associated with agents who have enabled ICD extensions.

Step 10   Click **Update** to apply the changes.

Step 11   Click **Insert**.

The Application Profile area of the User Information web page is now populated with the user name you entered. Device Association, Extension Mobility, and Softphone hyperlinks also appear.

Improving Cisco CallManager Performance under High Agent and Call Load

If you have installed Cisco CRA on a MCS-7845 server, the system can handle a high number of agents and heavy call load (up to 150 agents and 300 calls). However, Cisco CallManager performance degrades under high agent and call load if the default trace setting is used and AntiVirus is enabled, resulting in rejected and aborted calls.

You can improve Cisco CallManager performance under high load by performing the following steps.

Procedure

Step 1   Set Cisco CallManager SDL Trace Directory path to: F:\Program Files\Cisco\Trace\SDL\

Step 2   Set the Cisco CallManager SDL Trace output setting to file name: F:\Program Files\Cisco\Trace\CCM\ccm.txt

Step 3   Exclude the following folders from AntiVirus: C:\Program Files\Cisco\Trace and F:\Program Files\Cisco\Trace

Improving Cisco CallManager Performance under High Agent and Call Load

C H A P T E R **3**

Setting Up the Cisco IP Telephony Directory

Before setting up the Cisco IP Telephony Directory and administrator, complete the following tasks on Cisco CallManager:

- Create a JTAPI User, page 2-4
- Add CTI Ports, page 2-5
- Add CTI Route Points, page 2-6
- Associate Devices with the JTAPI User, page 2-8

The Cisco CRA system stores configuration information in a Lightweight Directory Access Protocol (LDAP) directory called the IP telephony directory. You can use the Cisco CallManager Data Connection (DC) directory as your IP telephony directory, or you can use an existing directory in your system (such as Netscape Directory or Microsoft Active Directory).

Configuring the directory server is typically a one-time process that you will never need to repeat, except in rare cases such as when you change the configuration or re-initialize a profile.

You can configure multiple directory servers, in order of priority, to be used if a failover occurs. Each of these directory servers stores Cisco CRA configuration data and scripts. If a failover occurs, the CRA server will attempt to use the first alternative directory server that you have configured, then the second server, and so on.

Note Each directory server must be in the same cluster for this failover to work.

The IP telephony directory contains a subdirectory that stores applications and Cisco scripts. This subdirectory is called the *repository*.

The CRA server can receive directory information from one IP telephony directory and application configuration and script logic from a repository on another server.

For efficient management of resources, the IP telephony directory server stores each type of configuration as a profile.

The CRA system uses two kinds of profiles:

- Configuration profile—Stores all the configuration for a specific CRA server, such as groups, triggers, and subsystems. A configuration profile can be used by only one CRA server at a time.

- Repository profile—Stores information common to multiple CRA servers, such as scripts and application configuration. A repository profile can be shared by multiple CRA servers.

Configuring the IP telephony directory server involves the following tasks:

1. Connect to the Cisco CRA Administration Web interface for the first time.

2. Set up the IP telephony directory.

3. Configure CRA administrators.

This chapter includes the following procedures:

Connecting to the Cisco CRA Administration Web Interface for the First Time

The CRA Administration web interface provides access to web pages that allow you to configure and administer the CRA system.

To connect to the CRA Administration web interface for the first time, complete the following steps.

Procedure

Step 1   Open the CRA Administration Authentication page by performing one of the following actions:

- From the server running Cisco CRA, choose **Start > Programs > Cisco CRA Administrator > Application Administrator**.

- From a web browser on any computer on your network, enter the following URL:

  http**://***servername*/AppAdmin

  In this example, *servername* is the host name or IP address of your Cisco CRA server.

Step 2   Enter `Administrator` in the User Identification field, enter `ciscocisco` in the Password field, and then click **Log O**n.

Use the specified login name and password during the first-time set-up process only. When you configure the Cisco IP telephony directory, you create a login name and password to use for future access to the CRA Administration web interface.

You are now ready to configure the IP telephony directory.

Setting up the IP Telephony Directory

Once you have logged into CRA Administration, you set up the IP telephony directory server.

You can use the Cisco CallManager DC directory as your IP telephony directory, or you can use an existing directory in your system (such as Netscape Directory or Microsoft Active Directory). See *Cisco Customer Response Applications Getting Started Guide* for sample values for configuring Netscape and Microsoft Active Directories.

Note   When you set up the IP telephony directory server, you set up repository and configuration profiles. If you change the profiles after initial setup, you must restart the CRA Engine.

To set up the IP Telephony Directory, complete the following steps.

Procedure

Step 1   After you have logged into CRA Administration for the first time, click **Setup**.

The Directory Setup web page opens, displaying the Configuration Setup—Step 1 of 6 area.

Step 2   From the Server Type drop-down menu, choose the type of LDAP directory you want to use—MS Active Directory, Netscape Directory Server 4.0, DC Directory, or Other.

The default information in the Directory User, Base Context, and User Base fields will differ according to the type of directory you choose.

Step 3   In the Directory Host Name field, enter the host name or IP address of the Cisco IP Telephony Directory server where the configuration profile resides or will reside with the CRA Engine profile. The information entered in this field should be consistent with the information entered in the CTI Manager A area on the CTI Manager Locations pane during CRA installation.

To specify multiple directory servers in the event of a failover, after you enter the primary host name or IP address, enter the host names or IP addresses of the alternative directory servers in the order that they should be used if a failover occurs. Separate each host name or IP address in the Directory Host Name field with a semicolon (;), a comma (,), or a space. The information entered in this field should be consistent with the information entered in the CTI Manager B area on the CTI Manager Locations pane during CRA installation.

Step 4   In the Directory Port Number field, enter the port number of the Cisco IP telephony directory.

The default is 8480.

Step 5   In the Directory User (DN) field, enter the username (called the distinguished name) configured on the directory server for the user with permission to modify the Cisco IP Telephony tree and object entries, or accept the default information.

Step 6   In the Directory Password field, enter a password for the directory user.

Step 7   In the Base Context field, enter the branch of the Cisco IP Telephony Directory tree that contains the Cisco configuration information, or accept the default information.

Step 8   In the User Base field, enter the branch of the Cisco IP Telephony Directory tree that contains user information, or accept the default information.

Step 9   Click **Next**.

The Configuration Setup—Step 2 of 6 area of the Directory Setup web page opens.

Step 10   In the Profile Name field, perform one of the following tasks:

- From the drop-down menu, choose the profile name that identifies this CRA server configuration or repository. The User Profile dialog box opens.

- Click **Edit.** The User Profile dialog box opens.

Step 11   Enter a new profile name, and then click **OK**.

The User Profile dialog box closes, and the new name opens in the Profile Name field of the Configuration Setup—Step 2 of 6 area of the Directory Setup web page.

If the profile you are using is a Cisco CRA 2.*x* profile, use the Cisco CRA conversion tool to convert it into a Cisco CRA 3.1 profile. For more information, see *Getting Started with Cisco Customer Response Applications*.

Step 12   Click **Next**.

The Configuration Setup—Step 3 of 6 area of the Directory Setup web page opens.

Step 13   Perform one of the following tasks:

- To create the repository profile on the same server as your configuration profile, accept the default setting (**Use the Default Repository Profile).**

- To maintain separate profiles for your configuration and repository, click the **Use a Different Repository Profile** radio button.

  The Repository Configuration dialog box opens.

  Complete the fields with configuration information appropriate for your repository directory, and then click **OK**.

  The Repository Configuration dialog box closes.

Step 14   Click **Next**.

The User Maintenance web page opens.

Step 15 If you want to find a specific Cisco CallManager user, enter search criteria (such as a user name) in the Enter Search Criteria text field and click **Search**.

If more than 75 users are configured on Cisco CallManager, you can search for users who are not displayed.

Step 16 From the CMUsers list box, select one or more Cisco CallManager users, and then click < to move the selected users to the CRA Administrator/Supervisor list box.

Step 17 For each user moved to the CRA Administrator/Supervisor list box, select a user in the list box and choose either Administrator or Supervisor from the Group drop-down menu.

Because only an administrator can update the CRA system, you must select at least one user to become an administrator.

Step 18 Click **Finish** to complete the process and initialize configuration and repository profiles.

The Directory Setup web page displays your configuration choices.

You are now ready to use the Cisco CRA Administration web interface to administer your CRA system.

Logging into CRA Administration

The CRA Administration web interface provides access to web pages that allow you to configure and administer the CRA system.

When you connect to the CRA Administration web interface for the first time, you perform a variety of setup procedures. (See Connecting to the Cisco CRA Administration Web Interface for the First Time, page 3-2.)

To connect to the Cisco CRA Administration web interface for the second time, and all subsequent times, you use the administrator username and password that you created while setting up the IP Telephony Directory.

To log in to CRA Administration, complete the following steps.

Procedure

Step 1   Open the CRA Administration Authentication page by performing one of the following actions:

- From the server running Cisco CRA, choose **Start > Programs > Cisco CRA Administrator > Application Administrator**.

- From a web browser on any computer on your network, enter the following URL:

  http**://***servername*/AppAdmin

  In this example, *servername* is the host name or IP address of your Cisco CRA server.

Step 2   Enter the administrator username and password you created and click **Log On**.

The initial login name (`Administrator`) and password (`ciscocisco`) are no longer valid.

The Cisco Application Administration web page opens.

Logging into CRA Administration

Provisioning Telephony and Media

Complete before provisioning telephony and media:

- Configure your Cisco CallManager to communicate with the Cisco CRA server (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

- Set up your IP telephony directory (see Chapter 3, "Setting Up the Cisco IP Telephony Directory.")

Now you need to provision and configure your Cisco CRA system. *Provisioning* is the process of allocating resources and devising strategies for drawing on them to support the needs of your business. *Configuring* is the process of making applications available to the CRA system.

Chapters 4 through 8 of this guide explain the process of provisioning the subsystems and configuring the applications of your CRA system. This chapter introduces the CRA telephony and media subsystems and explains how to provision resources for them.

The CRA system uses a telephony resource called Computer Telephony Interface (CTI) ports to accept incoming calls and to place outbound calls. The CRA system uses the following media resources to provide interactive services for calls:

- CMT (Cisco Media Termination)—The CMT media resource collects Dual Tone Multi-Frequency (DTMF) data from callers.

- Nuance ASR (Automated Speech Recognition)—The ASR media resource allows callers to use speech to navigate menus and to provide other information to CRA applications.

- Nuance TTS (Text-To-Speech)—The TTS media resource enables CRA applications to play back documents to callers as speech.

Note Previous releases of the Cisco CRA system automatically associated media resources with CTI ports. Cisco CRA 3.0 and 3.1 allow you to provision media resources independently from telephony resources. You can also provision the system to accept calls without media. (See .)

In CRA 3.0 and 3.1, media resources are licensed and sold as Cisco IP Interactive Voice Response (IVR) ports. Although you can provision more channels than you are licensed for, licensing is enforced at run-time. If more channels are provisioned than licensed, the system will not accept the extra calls, as doing so would violate your licensing agreements.

The CRA system uses the concept of *groups* to share telephony and media resources among different applications. *Call control groups* allow you to control how the system uses CTI ports. For example, you can reserve more ports for higher-priority applications or provide access to fewer ports for applications with less traffic. *Media resource groups* allow you to share media resources among different applications. For example, you can share ASR media resource groups with applications that collect caller information and applications that transfer calls to specific extensions.

The CRA system also uses the concept of *triggers*, which are specified signals that invoke application scripts in response to incoming contacts.

To provision telephony and media resources, perform the following tasks:

1. Provision the JTAPI subsystem.

    The Java Telephony Application Programming Interface (JTAPI) subsystem controls the telephony resources for the CRA system.

2. Provision the Cisco Media subsystem.

    The Cisco Media subsystem controls the CMT media resources for the CRA system.

    3. Provision the Nuance ASR subsystem.

    The Nuance ASR subsystem controls the ASR media resources for the CRA system.

    4. Provision the Nuance TTS subsystem.

    The Nuance TTS subsystem controls the TTS media resources for the CRA system.

You must be logged into the CRA Administration web interface to perform these tasks.

This chapter includes the following sections:

Provision the JTAPI Subsystem

The Java Telephony Application Programming Interface (JTAPI) subsystem is the subsystem of the CRA Engine that sends and receives call-related messages from the Cisco CallManager CTI Manager. To enable your CRA server to handle IP telephony requests, you will need to provision the JTAPI subsystem.

To provision the JTAPI subsystem, perform the following tasks:

    1. Configure a JTAPI Provider.

    You must specify the server on which the Cisco Media Convergence server (Cisco MCS) is running Cisco CallManager CTI Manager, and provide the user ID and password when you configured the JTAPI user in Cisco CallManager.

    2. Provision JTAPI call control groups.

    JTAPI call control groups pool together a series of CTI ports, which the system then uses to serve calls as they arrive at the CRA server.

    3. Provision a JTAPI trigger.

    JTAPI triggers invoke application scripts in response to incoming contacts.

This section contains the following procedures:

Configuring a JTAPI Provider

The JTAPI Providers area of the JTAPI Configuration web page allows you to specify the host name or IP address of the server running Cisco CallManager CTI Manager and specify the user ID and password that will allow Cisco CallManager to direct calls to the CRA server.

Note   Before you can provision the JTAPI subsystem, you must create a Cisco CallManager user for the JTAPI subsystem, create CTI ports and CTI route points, and associate the ports and route points with the JTAPI user. (See Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

To configure the JTAPI subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > JTAPI**.

The JTAPI Configuration web page opens.

Step 2   In the JTAPI Provider(s) field, enter the host name or IP address of the Cisco Media Convergence server (Cisco MCS) running Cisco CallManager CTI Manager.

You can enter up to two CTI Managers, separated by a space. If the first CTI Manager becomes unavailable, the second one connects and maintains calls.

Step 3   In the User ID field, enter the Cisco CallManager User ID.

You created this user ID when you configured the JTAPI user in Cisco CallManager. (See Create a JTAPI User, page 2-4.)

Step 4   In the Password field, enter the password.

You defined this password when you created the user in Cisco CallManager for the JTAPI subsystem. (See Create a JTAPI User, page 2-4.)

Step 5   Click **Update** to apply changes.

A dialog box opens, indicating that the JTAPI subsystem has been configured successfully.

Step 6   Click **OK**.

The dialog box closes and the system displays the JTAPI Configuration web page.

You are now ready to provision JTAPI call control groups.

Provisioning JTAPI Call Control Groups

The CRA system uses JTAPI call control groups to pool together a series of CTI ports, which the system uses to serve calls as they arrive at the CRA server. You can create multiple JTAPI call control groups in order to share and limit the resources to be used by specific applications.

Note   Before you can provision JTAPI call control groups, you must create a Cisco CallManager user for the JTAPI subsystem, create CTI ports and CTI route points, and associate the ports and route points with the JTAPI user. (See Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

Note   If your system is co-located with Cisco CallManager, you can configure a maximum of 256 CTI ports in total for all CTI port groups. Configuring more CTI ports than this limit results in calls being aborted by the system in an unspecified manner.:

To configure a JTAPI call control group, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > JTAPI**.

The JTAPI Configuration web page opens.

You can access the JTAPI Configuration web page only when the CRA Engine is running.

Step 2   On the JTAPI Configuration navigation bar, click the **CTI Port Groups** hyperlink.

The first JTAPI Call Control Group Configuration web page opens.

Step 3   Click the **Add a New JTAPI Call Control Groups** hyperlink.

The second JTAPI Call Control Group Configuration web page opens.

Step 4   In the **Group ID** field, accept the automatic group ID, or enter a group ID.

The Group ID corresponds to the trunk group number reported to the Intelligent Contact Management (ICM) when the CRA server is part of the Cisco IP Contact Center (IPCC) solution.

Step 5   Press the **Tab** key to automatically populate the Description field.

Step 6   From the **Calling Search Space for Redirect** drop-down list, choose the option that specifies the search space, or partition, the calling device searches when attempting to redirect the call.

Step 7   Click **Associate CTI Ports**.

The Please Assign CTI Ports for this Group web page opens. (Once you have assigned a CTI port to a group, the title of the Please Assign CTI Ports for this Group web page changes to the associated CTI port group number.

Step 8   From the Available CTI Port List Filters drop-down menus, choose **Device Name** and **Is Exactly**, and then click the **Find** button.

The Directory Number and Device Name of the CTI port appear under their respective columns.

Step 9   Check the check box in the row that contains the directory number of the CTI port.

Step 10   Click **Update** to add the port to the list of available CTI ports.

The second JTAPI Call Control Group Configuration web page opens.

Step 11   Click **Add**.

The first JTAPI Call Control Group Configuration web page opens. The call control group you have just added appears in the Group ID column. You are now ready to provision a JTAPI trigger.

Provisioning a JTAPI Trigger

You must configure JTAPI triggers to invoke application scripts in response to incoming contacts. A JTAPI trigger responds to calls that arrive on a specific route point by selecting telephony and media resources to serve the call and invoking an application script to handle the call.

To add and configure a JTAPI trigger, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > JTAPI**.

The JTAPI Configuration web page opens.

You can access the JTAPI Configuration web page only when the CRA Engine is running.

Step 2   On the JTAPI Configuration navigation bar, click the **JTAPI Triggers** hyperlink.

The first JTAPI Trigger Configuration web page opens. (Click the **Add a New JTAPI Trigger** hyperlink.

The second JTAPI Trigger Configuration web page opens.

Step 3   From the CTI Route Point Directory Number drop-down menu, choose an available CTI route point (directory number) to associate with the trigger.

Step 4   In the Language field, perform one of the following tasks:

- From the Language drop-down menu, choose the default language to associate with the incoming call when the application is started.

- Click the **Edit** button.

    The User Prompt dialog box opens.

    In the User Prompt dialog box, enter the name of the language, and then click **OK**.

    The User Prompt dialog box closes, and the name of the language opens in the Language field in the JTAPI Configuration web page.

Step 5   From the Application Name drop-down menu, choose the name of the application to associate with the trigger.

Step 6   In the Maximum Number of Sessions field, enter the maximum number of simultaneous calls that the trigger can handle.

Step 7   In the Idle Timeout (in ms) field, enter a value that specifies the number of milliseconds the system will wait before timing out.

In the Enabled field, click the **Yes** radio button to enable the trigger, or click the **No** radio button to disable the trigger.

Step 8   From the Call Control Group drop-down menu, choose the call control group to associate with the trigger.

Step 9   From the Primary Dialog Group drop-down menu, choose the dialog group to associate with the trigger (if media is required by the associated application).

Step 10   From the Secondary Dialog Group drop-down menu, choose a back-up dialog group to associate with the trigger if the primary dialog group does not have enough resources to provide for an incoming call on this trigger.

Step 11   Click **Add**.

The first JTAPI Trigger Configuration web page opens, showing the new JTAPI trigger.

You are now ready to provision the Cisco Media subsystem.

Provision the Cisco Media Subsystem

The Cisco Media subsystem is a subsystem of the CRA Engine. The Cisco Media subsystem manages the CMT (Cisco Media Termination) media resource, which collects Dual Tone Multi-Frequency (DTMF) data from callers.

The Cisco Media subsystem uses *dialog groups* to organize and share resources among applications. A dialog group is a pool of *dialog channels* in which each channel is used to perform *dialog interactions* with a caller, during which the caller responds to automated prompts by pressing buttons on a touch-tone phone.

To enable your CRA applications to handle simple DTMF-based dialog interactions with customers, you will need to provision the Cisco Media subsystem to configure CMT dialog groups.

To configure a CMT dialog group, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Subsystems > Cisco Media**.

The first Cisco Media Termination Dialog Group Configuration web page opens.

Step 2 Click the **Add a New CMT Dialog Control Group** hyperlink.

The second Cisco Media Termination Dialog Group Configuration web page opens.

Step 3 In the **Group ID** field, accept the automatic group ID, or enter a unique group ID.

This Group ID must be unique within all media group identifiers, including ASR group identifiers.

Step 4 Tab to the Description field to automatically populate the field.

Step 5 In the Maximum Number Of Channels field, enter the maximum amount of channels available for the group, based on your licensing agreement.

Step 6 Click **Add**.

The first Cisco Media Termination Dialog Group Configuration web page opens, showing the new CMT dialog group.

You are now ready to provision Nuance ASR and Nuance TTS subsystems.

Provision the Nuance ASR Subsystem

The Nuance ASR (Automated Speech Recognition) subsystem allows users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone. When a user calls local directory assistance, for example, ASR can prompt the user to say the city and state in which to locate the information, then connect the user to an appropriate operator.

To provision the Nuance ASR subsystem, you need to perform the following tasks:

1. Provision the ASR speech server. This server is the server on which the Nuance ASR system is installed.

2. Provision ASR dialog groups. ASR dialog groups allow CRA applications to use speech recognition.

This section contains the following topics:

- Provisioning the Nuance ASR Speech Server, page 4-10
- Provisioning Nuance ASR Dialog Groups, page 4-11

Provisioning the Nuance ASR Speech Server

The ASR speech server is the server on which the Nuance ASR feature is installed.

To provision the Nuance ASR speech server, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Subsystem > Nuance ASR**.

The first Nuance ASR Configuration web page opens.

Step 2 In the Speech Server Host Name(s) field, enter one or more speech server host names (separated by a space or comma).

Step 3 From the Refresh Frequency drop-down menu, choose a refresh frequency rate.

Use the Refresh Frequency option to determine how frequently the system refreshes. Refresh rates are: Never, Once, Daily, and Weekly.

Step 4   From the Refresh Task Start Time drop-down menu, choose a start time to refresh the scripts. For more information on refresh options, see The Nuance ASR Configuration Hyperlink, page 17-37.

Step 5   Click **Update** to apply changes.

Your changes appear in the Nuance ASR Configuration web page. You are now ready to provision Nuance ASR dialog groups.

If this is the first time that you have configured the ASR server on a new host machine, the Network Share Log-on Configuration web page opens.

The Network Share Log-on web page opens only when you configure an ASR server on a new host machine for the first time. After you configure the Network share, the web page will not appear when you add a new server on the same host machine.

Step 6   Enter a valid user name and password for the ASR server on which you have administrative privileges.

Step 7   Click **Go** to enable the network connection.

The system establishes the network connection to the speech server, and the first Nuance ASR Server Configuration web page opens.

Provisioning Nuance ASR Dialog Groups

If you are using Nuance ASR speech recognition, you must create at least one Nuance ASR dialog group to allow applications to use speech recognition.

To provision an ASR dialog group, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystem > Nuance ASR**.

The Nuance ASR Configuration web page opens.

Step 2   On the Nuance ASR Configuration navigation bar, click the **Nuance ASR Dialog Control Groups** hyperlink.

The second Nuance ASR Configuration web page opens.

Step 3   Click the **Add a New Nuance ASR Dialog Control Group** hyperlink.

The Nuance ASR Dialog Control Groups web page opens.

Step 4   In the Group ID field, enter a unique group ID.

This Group ID must be unique within all media group identifiers, including CMT group identifiers.

Step 5   Tab to the Description field to automatically populate this field.

Step 6   In the Maximum Number of Sessions field, enter the number of channels that the groups will define.

The number of channels corresponds to the maximum number of simultaneous calls this group can process.

Step 7   Click **Add** to apply changes.

The second Nuance ASR Configuration web page opens, showing the new Nuance ASR dialog group. You are now ready to provision the Nuance TTS subsystem.

Provision the Nuance TTS Subsystem

The Nuance Text-to-Speech (TTS) subsystem converts plain text (UNICODE) into spoken words in order to provide a user with information or prompt a user to respond to an action.

For example, a company may use TTS to prompt a customer to enter a name, address, and telephone number so that the company can ship a requested product to the customer's location. Or a customer may dial into a pre-designated phone number, access a voice portal, and listen to the latest weather report or stock quotes. TTS can also convert e-mail text to speech and play it back to the customer over telephone.

$\begin{aligned}&\diagdown\\&\diagdown\end{aligned}$

Note   Cisco CRA 3.1 supports the One-CRA-Server-to-Multi-TTS-Server feature.

To provision the Nuance TTS subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > Nuance TTS**.

The first Nuance TTS Server Configuration web page opens.

Step 2   Click the **Add New Nuance TTS Server** hyperlink.

The second Nuance TTS Server Configuration web page opens.

Step 3   In the ID field, enter an **ID** for the TTS Server.

The ID must be a unique integer.

Step 4   In the TTS Host Name field, enter the host name or IP address of the TTS server.

Step 5   In the TTS Port field, enter a port number.

This port number is the Transmission Control Protocol (TCP) port number that the CRA system uses to open a TCP socket to the TTS server. (The range is between 30000 and 32323).

An error occurs if you enter a value that is not within the specified range or if you enter a value that is not numerical.

Step 6   From the TTS Language drop-down menu, choose a language supported by the server.

Your CRA package determines the languages that are available to you.

Step 7   From the **Voice Gender** drop-down menu, choose a gender supported by the server.

Step 8   Click the **Update** button to apply changes.

A dialog box opens.

Step 9   Click **OK**.

The Network Share Log-on Configuration web page opens.

The Network Share Log-on web page opens only when you configure a TTS server on a new host machine for the first time. After you configure the Network share, the web page will not appear when you add a new server on the same host machine.

Step 10   Enter a valid user name and password for the speech server on which you have administrative privileges.

Step 11 Click **Go** to enable the network connection.

The system establishes the network connection to the speech server, and the first Nuance TTS Server Configuration web page opens.

Step 12 Restart the Engine.

(Follow the instructions described in the "Starting and Stopping the CRA Engine" section on page 14-14.)

Step 13 To set a voice speed, open Windows Explorer, and locate the TTS.properties file under the following path: **C:\Program Files\wfavvid**

Step 14 Right-click the file name.

The TTS.properties file opens. The last line of the file contains the default voice speed setting.

Step 15 Erase the current value and enter a new value to increase or decrease the voice speed.

The value for voice speed is between 1and 100. A higher value indicates a faster speed. The default voice speed setting is 50.

Step 16 Close the TTS.properties file.

You are now ready to provision other CRA subsystems, peripheral systems, and configure applications.

If you have purchased a Cisco IP ICD (Integrated Contact Distribution) package, your next task is to provision the ICD subsystem (see Chapter 5, "Provisioning Cisco IP ICD."). If not, you can now provision one or more of the remaining CRA subsystems (see Chapter 6, "Provisioning Additional Subsystems.".

Provisioning Cisco IP ICD

If you have purchased a Cisco IP ICD (Integrated Contact Distribution) package, you can provision the ICD subsystem of your Cisco CRA system.

Complete the following tasks before provisioning IP ICD:

- Configure a Resource Manager (RM) user on Cisco CallManager (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")
- Enable Cisco CallManager users for the ICD extension (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")
- Set up your IP telephony directory (see Chapter 3, "Setting Up the Cisco IP Telephony Directory.")
- Provision your telephony and media resources (see Chapter 4, "Provisioning Telephony and Media.")

This chapter introduces the Cisco ICD subsystem and explains how to provision it. (If you did not purchase a Cisco IP ICD package, you should now provision one or more of the remaining CRA subsystems.)

Provisioning the IP ICD subsystem involves the following tasks

1. Provisioning the RM JTAPI provider.
2. Creating resource groups.
3. Creating skills, if you are using either of the IP ICD enhanced packages.
4. Assigning agents to resource groups and skills.
5. Creating Contact Service Queues.

You must be logged into the CRA Administration web interface to perform these tasks.

This section contains the following topics:

About IP ICD

The Cisco CRA system uses the ICD subsystem as part of a Automatic Call Distribution (ACD) system to provide resource distribution and queueing to call centers.

Cisco IP ICD uses Contact Service Queues (CSQs) as the entities that route calls to your resources (agents). Each CSQ controls incoming Cisco IP ICD calls and determines where an incoming call is placed in the queue and to which agent the call is sent.

Each CSQ selects resources from an associated resource pool that you define. When an agent becomes available to take a call, the system chooses a queued call from one of the CSQs whose resource pool includes the agent, and routes that call to that agent.

The following licensing options are available for the Cisco IP ICD system:

- IP ICD Standard (designed for entry-level users)—Includes the steps necessary for creating basic ICD applications.

- IP ICD Enhanced (designed for enterprise-level users)—Includes all functions of IP ICD Standard, plus support for skills-based routing and priority queuing.

- IP ICD Enhanced with CTI (Computer Telephony Interface) Option (available only to ICD Enhanced customers)—Adds full IP Interactive Voice Response (IVR) support (except for Intelligent Contact Management [ICM] integration), including database integration, Voice eXtensible Markup Language (VoiceXML), HTML web integration, custom Java extensions, and e-Notification services.

Note   The IP ICD Enhanced package and the IP ICD Enhanced with CTI Option package are provisioned in the same way.

You can install the CRA system on an MCS-7845 server or a different server. If you install the CRA system on an MCS-7845 server, your IP ICD subsystem can support the following maximum number of agents, skills, and CSQs:

- 150 agents
- 100 skills
- 75 CSQs

If you install the CRA system on a different server, your IP ICD subsystem can support the following maximum number of agents, skills, and CQSs:

- 75 agents
- 50 skills
- 25 CSQs

Provisioning the RM JTAPI Provider

The Resource Manager (RM) of the Cisco IP ICD system is a component of the ICD subsystem. It uses a Cisco CallManager JTAPI user (called a JTAPI provider) to monitor agent phones, control agent states, and route and queue calls.

To provision the RM JTAPI provider for the ICD subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens, displaying the RM JTAPI Provider area.

Step 2   In the RM JTAPI Provider(s) field, enter the host name or IP address of the Cisco Media Convergence Server (Cisco MCS) running Cisco CallManager CTI Manager.

You can enter up to two CTI managers, separated by a comma. If the first CTI manager becomes unavailable, the second one connects and maintains calls as a backup.

Step 3   In the User ID field, enter your Cisco CallManager user ID.

You created this user ID (for example, "RM") when you configured the JTAPI user in Cisco CallManager. (See the "Create a JTAPI User" section on page 2-4.)

Step 4   In the Password field, enter the password you defined for this User ID.

You created this password when you configured the JTAPI user in Cisco CallManager. (See the "Create a JTAPI User" section on page 2-4.)

Step 5   Click **Update** to apply changes.

The following message appears:

RM Subsystem configured successfully.

Creating, Modifying, and Deleting Resource Groups

Resource groups are collections of agents that your CSQ uses to handle incoming Cisco IP ICD calls. To use resource group-based CSQs, you must specify a resource group.

This section describes:

Creating a Resource Group

To create a resource group, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2 On the ICD Configuration navigation bar, click the **Resource Groups** hyperlink.

The Resource Groups area opens.

Step 3 Click the **Add a New Resource Group** hyperlink.

The Resource Group Configuration area opens.

Step 4 In the Resource Group Name field, enter a resource group name.

Enter a name that identifies the resource group (for example, "Languages").

Step 5 Click **Add**.

The Resource Groups area opens, displaying the resource group name in the Resource Group Name column.

Modifying an Existing Resource Group Name

To modify a resource group name, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2 On the ICD Configuration navigation bar, click the **Resource Groups** hyperlink.

The Resource Groups area opens.

Step 3   In the Resource Group Name column, click the resource group that you want to modify.

The Resource Group Configuration area page opens.

Step 4   Type the name of the resource group in the Resource Group Name text field.

Step 5   Click **Update** to apply the modifications.

The Resource Groups area opens, displaying the modified resource group name in the Resource Group Name column.

Deleting a Resource Group

When you delete a resource group, the resource group is removed automatically from any agents and CSQs to which it was assigned. Before deleting a resource group, reassign agents or CSQs to different or new resource groups.

To delete a resource group, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Resource Groups** hyperlink.

The Resource Groups area opens.

Step 3   Click the **Delete** icon next to the name of the Resource Group that you want to delete.

A dialog box opens, warning that the resource group is about to be permanently deleted

Step 4   Click **Continue.**

The resource group is deleted.

Creating, Modifying, and Deleting Skills

Skills are customer-definable labels assigned to agents. The two IP ICD Enhanced packages can route incoming calls to agents who have the necessary skill or sets of skill to handle the call.

This section describes:

- Creating a Skill, page 5-7
- Modifying an Existing Skill Name, page 5-8
- Deleting a Skill, page 5-8

Creating a Skill

See About IP ICD, page 5-2 for the number of skills that you can create on your system.

To create a skill, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Skills** hyperlink.

The Skills area of the ICD Configuration web page opens.

Step 3   Click the **Add a New Skill** hyperlink.

The Skill Configuration area of the ICD Configuration web page opens.

Step 4   In the Skill Name field, enter a description of a relevant skill (for example, French).

Step 5   Click **Add**.

The Skills area of the ICD Configuration web page opens, showing the skill in the Skill Name column.

Modifying an Existing Skill Name

To modify a skill name, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Skills** hyperlink.

The Skills area opens.

Step 3   In the Skill Name column, click the skill that you want to modify.

The Skill Configuration area page opens.

Step 4   Type the name of the skill in the Skill Name text field.

Step 5   Click **Update** to apply the modifications.

The Skills area opens, displaying the modified skill name in the Skill Name column.

Deleting a Skill

When you delete a skill, the skill is removed automatically from any agents and CSQs to which is was assigned. Before deleting a skill, reassign agents or CSQs to different or new skills.

To delete a skill, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Skills** hyperlink.

The Skills area opens.

Step 3   Click the **Delete** icon next to the name of the skill that you want to delete.

A dialog box opens, warning that the resource group is about to be permanently deleted

Step 4   Click **Continue.**

The resource group is deleted.

Assigning Resource Groups and Skills to Agents

Agents that handle calls are also called resources. After you create a resource group, you can assign agents (resources) to that group. If you have either of the ICD Enhanced packages, you can add skills to agents once the skills have been created. You can also select the *competence level* of the agent(s) in assigned skills. Competence level indicates the agent's level of expertise in that skill (1 indicating beginner and 10 indicating expert).

You can assign resource groups and skills to agents either individually or in bulk. The bulk option enables you to assign many agents to the same resource group and/or skills at the same time. You can assign up to 50 skills to agents.

Once you have assigned agents to resource groups and skills (if you are using either of the ICD Enhanced versions), you can create a CSQ (see Creating, Modifying, and Deleting Contact Service Queues, page 5-13)

Note   If you change the agent's record in Cisco CallManager (for example, delete the agent or modify the ICD extension), update the ICD configuration in the CRA system by selecting **Subsystems > ICD > Resources hyperlink.** The Cisco CallManager agent information also is updated at 10-minute intervals on the ICD subsystem.

This section describes:

Assigning a Resource Group and Skills to an Individual Agent

To assign a resource group and skills to an individual agent, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Resources** hyperlink.

The Resources area opens.

Only agents or supervisors who have assigned ICD extensions are displayed in the list of resources in the Resources area. (For information on assigning ICD extensions, see Provisioning the RM JTAPI Provider, page 5-3.)

Step 3   Click the name of the agent in the Resource Name column.

The Resource Configuration area opens.

Step 4   From the Resource Group drop-down menu, choose a resource group.

Step 5   In the Automatic Available field, accept the default (**Enabled**) to automatically put the agent into the Available state after the agent finishes an ICD call and disconnects.

All calls routed through the system are considered ICD calls, including ICD calls transferred by agents. When a logged on agent in Ready, Not Ready, or Work state answers an ICD call, the agent's state is subject to the Automatic Available setting. (See Creating a Contact Service Queue, page 5-14.)

Step 6   If you have either of the ICD Enhanced packages:

a.   Assign skills by selecting one or more skills from the Unassigned Skills list and clicking **<** to add the skills to the Assigned Skills List**.** Remove skills by selecting one or more skills from the Assigned Skills List and clicking **>** to add the skills to the Unassigned Skills list. You can assign up to 50 skills to the agent.

b.   Assign the agent's competence level for a skill by selecting the skill from the Assigned Skills list and choosing a number from the Competence Level drop-down menu.

Step 7   Click **Update** to apply the changes.

The Resources area of the ICD Configuration web page opens, and the agent is now assigned to the resource group and skills (if skills were assigned).

Assigning Resource Groups and Skills to Agents in Bulk

To assign resource groups and skills to agents in bulk, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Assign Skills** hyperlink.

The Assign Skills area opens.

Only agents or supervisors who have assigned ICD extensions are displayed in the list of resources in the Resources area. (For information on assigning ICD extensions, see Provisioning the RM JTAPI Provider, page 5-3.)

Step 3   In the Resource Name column, check the check box next to each agent you want to assign to the same resource group and/or skills. You can check the **Select All** check box to select all agents.

Step 4   Click the **Add Skill** Hyperlink

The Add Skill area opens.

Step 5   To assign all selected agents to the same resource group, choose a resource group from the Resource Group drop-down menu.

Step 6   To assign skills:

    a.   Choose one or more skills from the Skills list and click < to add the skills to the Skills to Add List. Note that the Skills to Add list contains only skills to be added, not skills that the agents already have. You can assign up to 50 skills to agents.

    b.   Assign the agents' competence level for a skill by choosing the skill from the Assigned Skills list and choosing a number from the Competence Level drop-down menu.

Step 7   Click **Update** to apply the changes.

The Assign Skills area of the ICD Configuration web page opens, and the agents are now assigned to the resource group and skills (if skills were assigned).

Removing Skills from Agents in Bulk

To remove skills from agents in bulk, complete the following steps.

Note   If a resource is not assigned a skill you attempt to remove, the resource is not updated. However, the system will still generate an "Apply change to selected resource" message.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Assign Skills** hyperlink.

The Assign Skills area opens.

Only agents or supervisors who have assigned ICD extensions are displayed in the list of resources in the Resources area. (For information on assigning ICD extensions, see Provisioning the RM JTAPI Provider, page 5-3.)

Step 3   In the Resource Name column, check the check box next to each agent you want to remove from the same skills.

You can check the **Select All** check box to select all agents.

Step 4   Click the **Remove Skill** Hyperlink

The Remove Skill area opens.

Step 5   Remove skills by choosing one or more skills from the Skills list and clicking >
to move the skills to the Skills to Remove list. Note that the Skills list displays the
total number of skills configured for ICD, not just those skills assigned to the
selected agents.

Step 6   Click **Update** to apply the changes.

The Assign Skills area of the ICD Configuration web page opens, and the agents
are no longer assigned to the skills.

Creating, Modifying, and Deleting Contact Service Queues

The Contact Service Queue (CSQ) controls incoming Cisco IP ICD calls by
determining where an incoming call is placed in the queue and to which agent the
call is sent.

After you assign an agent to a resource group and/or skills, you need to configure
the CSQs.

You assign agents to a CSQ by associating a resource group or skills to the CSQ.
Agents in the selected resource group or skills are assigned to the CSQ.

You can assign up to 50 skills to a single CSQ.

Each agent can belong to up to 25 CSQs. To ensure that agents are not assigned
to more than 25 CSQs, click the Resources hyperlink in the ICD Configuration
web page, and select the Open Resources Summary Report hyperlink. The report
opens, listing each agent and the number of CSQs to which the agent belongs. If
the agent belongs to more than 25 CSQs, modify the CSQs' resource pool, or
modify the skills to which the agent is assigned.

Note   With the IP ICD Standard package, each agent can be assigned to only one CSQ.

This section describes:

Creating a Contact Service Queue

See About IP ICD, page 5-2 for the number of CSQs that you can create on your system.

To create a new CSQ and assign agents, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Contact Service Queues** hyperlink.

The Contact Service Queues area opens.

Step 3   Click the **Add a new Contact Service Queue** hyperlink.

The first Contact Service Queue Configuration area page opens.

Step 4   In the Contact Service Queue Name field, enter a Contact Service Queue name.

Create a meaningful name that is concise, yet easy to recognize (for example, LanguageExperts).

Step 5   Choose to enable or disable Automatic Work for agents assigned to this CSQ.

If you enable Automatic Work, agents automatically enter 'work' state after calls. If you disable Automatic Work, the agent enters either Not Ready or Ready state, depending on the agent's Automatic Available setting. (See Assigning a Resource Group and Skills to an Individual Agent, page 5-10.)

Step 6   From the **Resource Pool Selection Model** drop-down menu, choose **Resource Skills** to create a skills-based CSQ (available only if you are provisioning an IP ICD Enhanced package), or choose **Resource Group** to create a resource group-based CSQ.

Step 7   In the Service Level field, enter the target maximum time a call is queued before it is connected to an agent.

Step 8   In the Service Level Percentage field, enter the target goal for percentage of contacts that meet the service level.

For example, a call center that has a service level of 20 and a service level percentage of 80 percent has a goal of answering 80 percent of its calls within 20 seconds.

Step 9   Click **Next**.

The second Contact Service Queue Configuration area opens.

Step 10   From the Resource Selection Criteria drop-down menu, choose the selection criteria as follows:

- If you selected Resource Groups for the Resource Pool Selection Model on the previous page, choose from:

  - **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time.

  - **Linear**—Selects the next available agent with the highest priority, as determined by the agent order in the Resources list.

  - **Circular**—Selects the next available agent with the highest priority, based on the last agent selected and the agent order in the Resources list.

  - **Most Handled Contacts**—Selects the agent who has answered the most handled calls.

  - **Shortest Average Handle Time**—Selects the agent who generally spends the least amount of time talking to customers.

- If you selected Resource Skills for the Resource Pool Selection Model on the previous page, choose from:

  - **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time.

  - **Most Handled Contacts**—Selects the agent who has answered the most handled calls.

  - **Shortest Average Handle Time**—Selects the agent who generally spends the least amount of time talking to customers.

- **Most Skilled**—Used for expert agent call distribution. Selects the agent with the highest total competency level and who has been available for the longest amount of time. The total competency level is determined by adding the agent's competency level in each assigned skill.

- **Least Skilled**—Used for expert agent call distribution. Selects the agent with the lowest total competency level and who has been available for the longest amount of time. The total competency level is determined by adding the agent's competency level in each assigned skill.

Step 11   Depending on the Resource Pool Model you selected on the previous page, either:

- Choose the resource group for this CSQ from the Resource Group drop-down menu.

- Choose the skills for this CSQ by choosing one or more skills from the Unassigned Skills list and click > to add the skills to the Assigned Skills list. Choose the minimum competence level for each skill by choosing the skill and choosing a number from the Minimum Competence drop-down menu.

Step 12   Click **Show Resources** to show all agents who meet the specified criteria.

The Resources list is populated with the list of agents who meet the specified criteria. If no agents display in this list, the specified criteria is too strict. Modify the criteria.

If you selected Most Skilled or Least Skilled as the Resource Selection Criteria, the agents appear in order based on total competency level.

If you selected Linear or Circular as the Resource Selection Criteria, arrange agents as needed in the Resources list by choosing an agent and using the up and down arrows to move the agent in the list. The order of the agents determines the priority, the agent at the top of the list having the highest priority.

Step 13   Click **Add** to apply changes and update the system.

The new CSQ is now displayed, and all agents who belong to the resource group or skill groups selected are now a part of this CSQ.

Modifying an Existing CSQ

You can modify existing CSQs. If you make dynamic configuration changes that affect the order in which agents receive ICD calls, the changes take effect when all agents affected by the changes have left the Ready state. If no agents are in the Ready state when you modify the CSQ, the changes take effect immediately.

To modify an existing CSQ, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Contact Service Queues** hyperlink.

The Contact Service Queues area opens.

Step 3   In the Name list, click the CSQ that you want to modify.

The first Contact Service Queue Configuration area page opens.

Step 4   Modify the CSQ as necessary.

Step 5   Click **Update** to apply the modifications.

Deleting a CSQ

When you delete a CSQ, any skills or resource groups assigned to that CSQ are automatically removed from the CSQ, and any application using that CSQ can no longer access it. Before deleting the CSQ, change the applications to use a different CSQ. If the application is using a CSQ when the CSQ is deleted, new incoming calls will get an error and existing queued calls will not be routed to agents. To delete a CSQ, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICD**.

The ICD Configuration web page opens.

Step 2   On the ICD Configuration navigation bar, click the **Contact Service Queues** hyperlink.

The Contact Service Queues area opens.

Step 3   Click the **Delete** icon next to the name of the CSQ that you want to delete.

Provisioning Additional Subsystems

These tasks must be complete before you provision additional subsystems:

- Configure your Cisco CallManager to communicate with the Cisco CRA server (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")
- Set up your IP telephony directory (see Chapter 3, "Setting Up the Cisco IP Telephony Directory.")
- Provision your telephony and media resources (see Chapter 4, "Provisioning Telephony and Media.")

If you purchased a Cisco IP Integrated Contact Distribution (ICD) package, you must also:

- Provision your ICD subsystem (see Chapter 5, "Provisioning Cisco IP ICD.")

If you plan to run applications that use any of the additional CRA subsystems included in your CRA package, you should now provision those subsystems. The CRA system uses these additional subsystems to communicate with supporting systems such as Cisco IP Contact Center (IPCC), web servers, database servers, and e-mail servers.

Note You need to provision a particular subsystem only if you are using CRA applications that require it.

Your CRA system may include some or all of the following additional subsystems:

- The ICM subsystem—The Cisco CRA system uses the ICM (Intelligent Contact Manager) subsystem to communicate with Cisco ICM, which is used by Cisco IPCC to manage call distribution across sites and call-processing environments.

- The HTTP subsystem—The Cisco CRA system uses the HTTP subsystem to enable CRA applications to respond to requests from a variety of web clients, including computers and IP phones.

- The Database subsystem—The Cisco CRA system uses the Database subsystem to enable CRA applications to interact with database servers in order to make database information accessible to contacts.

- The eMail subsystem—The Cisco CRA system uses the eMail subsystem to communicate with your e-mail server and enable your applications to create and send e-mail.

This chapter introduces each of these Cisco CRA additional subsystems and explains how to provision it. You must be logged into the CRA Administration to provision the subsystems.

This chapter includes the following procedures:

Provision the ICM Subsystem

The Cisco CRA system uses the ICM subsystem to communicate with Cisco Intelligent Contact Manager (ICM), which is used by Cisco IP Contact Center (IPCC) to manage call distribution across sites and call-processing environments.

The CRA server is frequently used as part of an IPCC solution with Cisco ICM. In this type of installation, the Cisco ICM uses the CRA server to queue calls and perform other functions such as collecting caller-entered digits, performing database lookups, and playing back prompts.

Note   If you are not using Cisco IPCC, you do not need to provision the ICM subsystem.

Cisco ICM scripts can direct calls based on various criteria such as the time of day or the availability of subsystems. The scripts use four different commands to interact with the CRA system:

- **Connect**—Connects the call. Cisco ICM sends the connect message with a label to instruct the CRA system where to direct the call.

- **Release**—Hangs up the call.

- **Run VRU Script**—Runs an ICM VRU (Voice Response Unit) script on the CRA system.

- **Cancel**—Cancels the ICM VRU script that is currently running.

To provision the ICM subsystem, you will need to perform the following tasks:

1. Configure general ICM information. General ICM information includes the TCP/IP socket number for receiving messages from the Cisco ICM system and the expanded call variables you want to use to pass call-related information.

2. Configure ICM VRU scripts. Cisco IPCC uses VRU scripts to handle interactions with contacts. These scripts are loaded as applications on the CRA Engine.

This section includes the following procedures:

Configuring General ICM Information

To configure general ICM information, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICM**.

The ICM Configuration web page opens, displaying the General area.

Step 2   In the VRU Connection Port field, enter the same number that is configured in the VRU peripheral interface manager (PIM) on the Cisco ICM system.

The system uses this TCP/IP socket number for receiving messages from the Cisco ICM system. You can copy the VRU Connection Port value from the VRU PIM configuration dialog box of the VRU peripheral gateway (PG) machine.

The default value in the Cisco ICM setup is 5000.

Step 3   In the Service Control field, click the **Yes** radio button.

The Service Control interface allows Cisco ICM to provide call-processing instructions to the Cisco CRA system. It also provides Cisco ICM with event reports indicating changes in call state.

You must enable the service control interface to use the ICM subsystem.

Step 4   In the Parameter Separator field, enter the character used to delineate individual parameters in a multiple parameter variable.

Step 5   In the Additional VRU Call Information check boxes, check the expanded call variables you want to use to pass call-related information. (See Table 6-1.)

Step 6   Click **Update**.

The configuration information is added to the system.

You are now ready to configure the ICM VRU Scripts area of the ICM Configuration web page.

Table 6-1   Expanded Call Variables

Expanded Call Variable	Description
Task ID	Task ID that handles the current call.
Media ID	Media ID that handles the current call.
Last Redirected Address	Transient part ID of the call.
Arrival Type	Arrival type of the call.
Session Handled	Boolean flag that the Cisco ICM or a Set Contact Info step with a Handled flag step sets to indicate whether the session is handled. **Note** Cisco CRA automatically sets the flag whenever a call is connected to an agent.
VRU Script Name	Script name to run on the PreConnect feature.
Config Param	Parameters for the VRU scripts on the PreConnect feature.

Note   You can also define your own expanded call variables with the Configure ICM tool in the Cisco ICM system. The CRA Engine registers the user-defined expanded call variables with Cisco ICM after it loads the VRU scripts that use these variables. The variables remain registered until the Cisco ICM session is reopened (either by request from the VRU peripheral gateway or when the CRA Engine is restarted). The variables remain registered even if you delete the script that uses them.

Configuring ICM VRU Scripts

Cisco IPCC uses Voice Response Unit (VRU) scripts to handle interactions with contacts. These scripts are loaded as applications on the CRA Engine.

To configure ICM VRU Scripts, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > ICM**.

The ICM Configuration web page opens, displaying the General area.

Step 2   On the ICM Configuration navigation bar, click the **ICM VRU Scripts** hyperlink.

The first ICM VRU Scripts area of the ICM Configuration web page opens.

Step 3   Click the **Add a New VRU Script** hyperlink.

The second ICM VRU Script area of the ICM Configuration web page opens.

Step 4   In the VRU Script Name field, enter a name for the VRU script you want to add.

Step 5   In the Script field, perform one of the following tasks:

- From the Script drop-down menu, choose the CRA script that you want to associate with the VRU script.

- Click the **Edit** button.

  The User Prompt dialog box opens.

  Enter the name of the script, and then click **OK**.

  The User Prompt dialog box closes, and the name you entered appears in the Script field.

Step 6   Click **Add**.

The second ICM VRU Script area closes, and the name of the VRU script you added appears in the first ICM VRU Scripts area.

You are now ready to provision any additional subsystems your CRA applications require or to begin configuring CRA applications. (See Chapter 7, "Configuring Cisco Script Applications.")

Provision the HTTP Subsystem

The Cisco CRA system uses the HTTP subsystem to enable CRA applications to respond to requests from a variety of web clients, including computers and IP phones.

Note If you are not using HTTP applications, you do not need to provision the HTTP subsystem.

The CRA system uses subdirectories in the Cisco CRA installation directory to store text substitution, xsl (eXtensible Style Language) templates, static and dynamic web pages, and Java Servlet Pages (JSPs).

The default installation directory for the CRA system is C:\program files\wfavvid.

The CRA system uses the following subdirectories of the installation directory to administer the HTTP subsystem:

- \template—Recommended for storing text substitution, xsl templates, and dynamic web pages.
- \tomcat—Stores the Tomcat server (developed by the Apache server development organization), the Java servlet that is the default web server included with the HTTP subsystem.
- \tomcat\ROOT—Stores static web pages and JSPs.

You can create additional subdirectories for different web sites or applications. It is possible to save static pages in any location to which the Tomcat server has access as long as it has adequate security to prevent unauthorized access.

To provision the HTTP subsystem, you need to provision HTTP triggers. HTTP applications use triggers to activate the application in response to an incoming HTTP message.

If necessary, you can change the TCP/IP port used by the HTTP server.

This section describes:

Configuring HTTP Triggers

To configure HTTP triggers for applications, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > HTTP**.

The first HTTP Trigger Configuration web page opens.

Step 2   Click the **Add a New HTTP Trigger** hyperlink.

The second HTTP Trigger Configuration web page opens.

Step 3   In the URL field, enter the URL that will be associated with the HTTP application.

The URL must be entered as /*myapp*, where *myapp* is the URL of the application. The URL can not contain any spaces, special characters, or backslashes.

Step 4   In the Language field, perform one of the following tasks:

- From the Language drop-down menu, choose the default language to be associated with the incoming HTTP request contact.

- Click **Edit**.

  The User Prompt dialog box opens.

  Enter the locale string for the language, and then click **OK**.

  The User Prompt dialog box closes, and the language you entered appears in the Language field.

Step 5   From the Application Name drop-down menu, enter the name of the application for which you are adding an HTTP trigger.

Step 6   In the Maximum Number Of Sessions field, enter the maximum simultaneous instances of the application that can run when triggered by this particular HTTP trigger.

Step 7   In the Idle Timeout (in ms) field, enter the maximum length of time the system will waits before rejecting the HTTP request for this trigger.

Step 8   In the Enabled field, click the **Yes** radio button to enable the HTTP trigger.

Step 9   Click **Add**.

The second HTTP Trigger Configuration web page closes, and the name of the VRU script you added appears in the first HTTP Trigger Configuration web page.

You are now ready to provision any additional subsystems your CRA applications require or to begin configuring CRA applications. (See Configuring Cisco Script Applications, page 7-1.)

Changing Port Numbers

You can set the TCP/IP port number the CRA Engine uses for the internal HTTP server when you install the HTTP subsystem. The default port used during installation is port 8080.

After the HTTP subsystem is installed, you can change the port in the Tomcat server.xml file.

To change the TCP/IP port number, complete the following steps.

Procedure

Step 1   Create a backup copy of the following configuration file:

installation directory\tomcat\conf\server.xml

Step 2   Open the original configuration file using any text editor.

Step 3   Search the file to find the string "Normal HTTP."

The following example shows the portion of the file that contains the port number:

<!-- Normal HTTP -->

    <Connector

className="org.apache.tomcat.service.PoolTcpConnector">

value="**8080**"/>

</Connector>

Step 4   Change the value 8080 to the port number you want to use.

The standard port number for HTTP is port 80. The default port number for SSL servers (HTTPS) is 443.

Step 5   Save the configuration file.

Step 6   Restart the CRA Engine by either:

- Choosing **System > Engine** from the CRA Administration menu bar.

    The Engine status page opens.

    Click **Stop Engine**. When the CRA Engine has stopped, click **Start Engine**.

- Restarting the CRA Engine from the Windows Service window, which you can open by choosing **Start > Programs > Administrative Tools > Services** from the Windows Start menu.

Provision the Database Subsystem

The Cisco CRA system uses the Database subsystem to enable CRA applications to interact with database servers in order to make database information accessible to contacts.

Note   If you are not using CRA applications that require access to databases, you do not need to provision the Database subsystem.

The following Enterprise Databases are supported for the Database subsystem:

- Microsoft SQL Server 7
- Microsoft SQL Server 2000
- Oracle 8i
- Oracle 9i
- Sybase Adaptive Server 12
- IBM DB2 7.2

To provision the Database subsystem, you will need to perform the following tasks:

1. Define an OBDC (Open Database Connectivity) datasource. The ODBC datasource name provides information to Microsoft Windows about how to connect the application server to an enterprise database such as Microsoft SQL Server, Sybase, Oracle, or IBM DB2.

2. Add a new datasource. After you define the OBDC datasource, you need to add this datasource to the Database subsystem.

This section includes the following procedures:

- Defining an OBDC Datasource, page 6-11
- Adding a New Datasource, page 6-13

Defining an OBDC Datasource

Before an application script can use information from a database, you must define an Open Database Connectivity (ODBC) datasource name. This name provides information to Microsoft Windows about how to connect the application server to an enterprise database such as Microsoft SQL Server, Sybase, Oracle, or IBM DB2.

To set up a datasource name, complete the following steps.

Procedure

Step 1   On the script server, choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.

The ODBC Data Source Administrator window opens.

Step 2   Click the **System DSN** tab.

The System DNS tab of the ODBC Data Source Administrator window opens.

Step 3   To add a Data Source Name (DSN), click **Add**.

The Create New Data Source window opens.

Step 4   Select the driver for which you want to set up a datasource, and click **Finish**. As an example, to create a DSN for Microsoft SQL Server, select **SQL Server.**

The Create a New Data Source to SQL Server window opens.

Step 5   In the Create a New Data Source to SQL Server window, perform the following tasks:

- In the **Name** field, enter a name.

  The name you enter must match the value entered in the Data Source Name field in the CRA Administration web interface.

- In the **Description** field, enter a description.

  Enter information that will help the application designer identify the purpose of this data source.

- From the **Server** drop-down menu, choose the host name or IP address of the computer where the enterprise database resides.

Step 6   Click **Next**.

The second Create a New Data Source to SQL Server window opens.

Step 7   Click the radio button of the appropriate authentication method: Windows NT or SQL Server.

Step 8   Click **Client Configuration** to configure the connection between the CRA server and the computer where the enterprise database resides.

The Client Configuration window opens.

Step 9   Choose **TCP/IP network libraries**.

Step 10   Enter a username in the Login ID field and a password in the Password field.

Make a note of the username and password you choose. You will use this username and password to complete the enterprise database configuration in the following procedure.

Step 11   Click **Next** to complete the DSN configuration and to test connectivity to the chosen data source.

You are now ready to add a new datasource.

Adding a New Datasource

After defining the OBDC datasource (see Defining an OBDC Datasource, page 6-11), you need to add this datasource to the Database subsystem.

To add a new datasource, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Subsystems > Database**.

The first Enterprise Database Subsystem Configuration web page opens.

Step 2 Click the **Add** a **New Datasource** hyperlink.

The second Enterprise Database Subsystem Configuration web page opens.)

Step 3 In the Data Source Name field, enter the name of the ODBC datasource.

Step 4 In the Username field, enter a username for connecting to the enterprise database.

Step 5 In the Password and Confirm Password fields, enter a password for connecting to the enterprise database.

Step 6 In the Maximum Number of Connections field, enter the maximum number of simultaneous connections allowed to connect to the database.

Step 7 Click **Add** to apply changes.

The first Enterprise Database Subsystem Configuration web page opens, showing the data source you added. You are now ready to provision any additional subsystems your CRA applications require or to begin configuring CRA applications. (See Configuring Cisco Script Applications, page 7-1.)

Provision the eMail Subsystem

The CRA system uses the eMail subsystem to communicate with your e-mail server and enable your applications to create and send email. You must provision the eMail subsystem if you intend to create scripts that use messaging steps to create and send e-mail.

Note   If you are not using eMail applications, you do not need to provision the eMail subsystem.

The e-mail configuration process identifies the default e-mail address and server to be used for sending e-mail (including e-pages and faxes) and for receiving acknowledgments.

To provision the eMail subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > eMail**.

The eMail Configuration web page opens.

Step 2   In the Mail Server field, enter the fully-qualified e-mail server name (for example, server.domain.com).

Step 3   In the eMail Address field, enter the existing fully qualified e-mail address for the administrative account (for example, administrator@domain.com).

This e-mail account must already exist on the mail server.

Step 4   Click **Update**.

The Cisco CRA system saves your changes and the CRA Administration web page opens.

Cisco does not currently support multiple e-mail configurations. To remove the e-mail information, you must erase the fields and click **Update**.

You are now ready to provision any additional subsystems your CRA applications require, or to begin configuring CRA applications. (See Chapter 7, "Configuring Cisco Script Applications," and Chapter 8, "Configuring Additional CRA Applications."

Configuring Cisco Script Applications

Complete the following tasks before configuring CRA applications:

- Configure your Cisco CallManager to communicate with the Cisco CRA server (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

- Set up your IP telephony directory (see Chapter 3, "Setting Up the Cisco IP Telephony Directory.")

- Provision your telephony and media resources, including provisioning the system to handle JTAPI calls and HTTP requests (see Chapter 4, "Provisioning Telephony and Media.")

- Provision your Integrated Contact Distribution (ICD) subsystem, if necessary (see Chapter 5, "Provisioning Cisco IP ICD.")

- Provision any additional subsystems your CRA applications will require (see Chapter 6, "Provisioning Additional Subsystems.")

You must now configure the CRA applications you intend to use. The Cisco CRA system uses applications to interact with contacts and perform a wide variety of functions, such as prompting callers for information, transferring calls, and providing information to callers.

This chapter introduces Cisco CRA *script* applications, which are applications based on scripts created in the CRA Editor. (For more information on using the CRA Editor to create scripts, refer to the *Cisco Customer Response Applications Developer Guide*.)

You can use the CRA Editor to create scripts that direct the CRA system to automatically answer calls and other types of contacts, prompt callers for information, accept caller input, queue calls, distribute calls to available agents, place outbound calls, respond to HTTP requests, and send e-mail messages.

(For information on configuring other types of Cisco CRA applications, see Chapter 8, "Configuring Additional CRA Applications.")

Note   The Cisco CRA package includes a number of sample scripts. For a description of these sample scripts, and for more information on creating scripts with the CRA Editor, refer to the *Cisco Customer Response Applications Developer Guide*.

Cisco script applications can make use of many components, such as scripts, pre-recorded prompts, grammars, and custom Java classes. You must first make these components available to the CRA Engine before you can configure a Cisco script application that uses them.

Depending on your particular CRA implementation, you may need to perform most or all of the following tasks to configure a Cisco script application:

1. Manage scripts. Cisco script applications are based on scripts that you must upload to the repository and make available to the CRA system.

2. Manage prompts. Many applications make use of pre-recorded prompts, stored as .wav files, which are played back to callers in order to provide information and elicit caller response. You must upload these .wav files to the repository and make them available to the CRA system.

3. Install grammars. The CRA system uses specific grammars to recognize and respond to caller response to prompts. You must store these grammars in a directory to make them available to the CRA system.

4. Install customized CRA languages. Language packs, such as American English, Canadian French, and so on, are installed with Cisco CRA. You install language packs in a directory accessible by the CRA system.

5. Install Java files. In addition to the Java files automatically installed as part of the Cisco CRA installation process, you can install your own custom classes and Java Archive (JAR) files in order to customize the performance of your CRA system.

6. Add a Cisco script application. Scripts created in the CRA Editor are used as the basis for Cisco script applications.

7. Add an application trigger. Triggers are specified signals that invoke application scripts in response to incoming contacts. After adding a new Cisco script application, you need to add a trigger so that this application can respond to telephone calls and/or HTTP requests.

You must be logged into the CRA Administration web interface to perform most of these tasks.

This chapter includes the following procedures:

Manage Scripts

Scripts are created with the CRA Editor, and can perform a wide variety of functions. For example, scripts can prompt callers for extension numbers in order to transfer calls, place callers in a queue and route calls to available agents, and place outbound calls.

You can add, modify, and delete a script by choosing Script menu options from the menu bar of the Cisco CRA Administration web interface. (For more information on Script menu options, see Chapter 16, "The Scripts Menu.")

This section contains the following procedures (which can be performed in any order):

Adding a Script

To make a script available for use as a CRA application, you must first upload the script to the repository.

To upload a script to the repository, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2 Click the **Add a Script** hyperlink.

The **Uploading Scripts** window opens.

Step 3 In the Source Script Name field, click **Browse.**

A Choose File window opens.

Step 4 Navigate to the directory in which scripts are located, select a script, and then click **Open**.

The Choose File window closes, and the script path appears in the Source Script Name field.

Step 5 Click the Description Script Name field to automatically enter the script name.

Step 6 Click **Upload to Repository** to upload the script to the repository.

A window opens, informing you that the script was successfully uploaded.

Step 7 Perform one of the following tasks:

- If the script is already being used by a CRA application, click the **Do You Want to Refresh the Script?** hyperlink, and then click **Yes** when the system prompts you to confirm the operation.

  When you refresh a script, you copy it from the repository to the CRA server, in order to make it available to the Cisco script application. (If the script does not already exist on the server, you do not need to refresh it.)

- If the script does not already exist on the CRA server, click the **Return to Script Management** hyperlink

  The Successful Script Upload window closes.

You are now ready to manage any existing scripts shown in the Script Management web page (if necessary) or add prompts that may be useful to your applications. (See Manage Prompts, page 7-10.)

Viewing or Downloading a Script File

You can view or download any script file that appears in the list on the Manage Scripts web page.

To view or download a script file, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2   In the row that contains the script file to view or download, click any information in the Name, Last Modified, or Created fields.

The File Download dialog box opens.

Step 3   Perform one of the following tasks:

- To view the script file, click **Open**.

  The script file opens in the CRA Editor.

- To download the script file, click **Save**, and then follow the prompts to choose a directory and file name for the script file.

  The file is saved to the specified directory.

Refreshing a Script

When you make changes to a script, you must refresh the script in order to direct all the applications and subsystems that use this script to reload the new version.

To refresh a script, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2 In the row that contains the script to refresh, click the Refresh icon.

The Refresh Script area opens, giving you the option of refreshing the script and the applications that reference it, or just refreshing the script.

Step 3 Perform one of the following actions:

- If you want all applications and subsystems that reference the script to use the new version, click **Yes.**

- If you do not want all applications and subsystems to use the new script, click **No** to refresh the script only.

The Manage Script web page opens, and the script appears in the list of scripts.

To refresh all scripts with one command, complete the following steps.

Procedure

Step 1   From the CRA Administration main menu, choose **Scripts > Refresh Scripts**.

An Engine web page opens, with a dialog box asking whether you would like to reload all applications as well as all scripts.

Step 2   Click **OK** to reload all applications as well as scripts, or click **Cancel** to reload scripts only.

A message appears in the Engine web page, informing you that the server has reloaded all scripts. (If you clicked **OK**, you are also informed that the server has reloaded all applications.)

Restoring a Script

When you restore a script, you replace the version currently in the repository with the previous version of the script.

Restoring a script is similar to using an Undo command. You can, for example, use the restore function when you make changes to a script, and then decide to use the previous version of the script instead.

To restore a script, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2   In the row that contains the script to restore, click the Restore icon.

A web page opens, indicating that the script was restored successfully.

Step 3   Perform one of the following tasks:

- If you want to continue configuring scripts without refreshing the script that you just restored, click the **Return to Script Management** hyperlink.

- If you want to refresh the script you just restored, follow these steps:

  - Click the **Do You Want to Refresh the Script?** hyperlink.

    An area opens, giving you the option of refreshing the script and the applications that reference it, or just refreshing the script.

  - Click **Yes** to refresh the script and all applications that reference it, or click **No** to refresh the script only.

The Script Management web page opens.

Uploading a Script

Use the Upload command to copy the latest version of a script to the repository.

To upload a script, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2   In the row that contains the script to upload, click the Upload icon.

The Upload Script window opens.

Step 3   In the Source Script Name field, click **Browse.**

A Choose File window opens.

Step 4   Navigate to a source file on your system, select the source file, and then click **Open**.

The script path appears in the Source Script Name field.

Step 5   Click **Upload to Repository**.

If you entered a file name in the Source Script Name field that differs from the name in the Destination Script Name field, the system prompts you for permission to continue. Click **OK** to continue, or click **Cancel** to enter a different name in the Source Script Name field.

A window opens, indicating that the script was uploaded successfully.

Step 6   Perform one of the following tasks:

- If you want to continue managing scripts without refreshing the script that you just restored, click the **Return to Script Management** hyperlink.

- If you want to refresh the script you just restored, follow these steps:

  – Click the **Do You Want to Refresh the Script?** hyperlink.

     An area opens, giving you the option of refreshing the script and the applications that reference it, or just refreshing the script.

  – Click **Yes** to refresh the script and all applications that reference it, or click **No** to refresh the script only.

The Script Management web page opens.

Deleting a Script

When you delete a script, you remove it permanently from the repository.

To delete a script, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Scripts > Manage Scripts**.

The Manage Scripts web page opens.

Step 2   In the row that contains the script to delete, click the Delete icon.

A dialog box opens asking you to confirm that you want to delete the script.

Step 3   Click **OK** to delete the script.

The dialog box closes and the Manage Scripts web page refreshes, now minus the deleted script.

Manage Prompts

Prompts are messages that the CRA system plays back to callers. Cisco script applications often use prompts to elicit caller response so that the Cisco CRA system can transfer calls, receive account information, and perform other functions.

To use prompts in your Cisco script applications, you must first create a folder to store them. You can then record and upload new user prompts, delete prompts, and modify existing prompts.

You store pre-recorded prompts as .wav files. The CRA system also allows users to record spoken names, which you can upload to be used in the playback of prompts.

Managing prompts involves the following tasks:

1. Create a folder to store prompts. You must create a folder to store the .wav files that the CRA system uses as prompts.

2. Record a prompt. You can record your own prompts to be used in applications.

3. Add a prompt. You must add prompts to the prompt subdirectory to make them available to Cisco script applications.

4. Upload a prompt. You can replace any of the stored prompts used by Cisco script applications with a different .wav file by uploading the new .wav file.

5. Add spoken name prompts. Some Cisco script applications play back the pre-recorded names of the people that callers are trying to reach, in order to allow the caller to confirm the transfer of the call.

6. Add multiple prompts. In addition to adding .wav files individually, you can add multiple .wav files at one time.

This section contains the following topics:

Creating a Folder to Store Prompts

You must create a folder to store the .wav files that the CRA system uses as prompts.

To create a new folder to store your prompts, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Tools > Prompt Management**.

The Prompt Management web page opens.

Step 2 From the Language Directory drop-down menu, choose a directory in which to create the folder.

Step 3 Click **Create Folder**.

The Create a New Folder window opens.

Step 4 In the Folder Name field, enter a folder name.

Step 5 Click **Create**.

The Prompt Management web page opens, displaying the new folder in the Language Directory drop-down menu.

You are now ready to record new prompts, if necessary, and add them to the new folder.

Recording a Prompt

You can record your own prompts to be used in applications.

The following procedure describes recording prompts with Microsoft Sound Recorder, using a microphone plugged into your computer.

The choices that you make when saving the prompt recording depend on whether you chose the G.711 or G.729 codec during CRA server installation.

> **Note**   If you are not using Microsoft Sound Recorder, refer to the documentation provided with your audio application.

To record a prompt, complete the following steps.

Procedure

Step 1   From your Windows Start menu, choose **Start > Programs** > **Accessories** > **Entertainment** > **Sound Recorder**.

The Sound Recorder dialog box opens.

Step 2   Click the **Record** button and speak your greeting into the microphone.

Step 3   Click the **Stop** button when you finish recording.

Step 4   To check your greeting, click the **Rewind** button or drag the slider back to the beginning of the recording. Then click the **Play** button.

Step 5   When you are satisfied with your greeting, choose **File > Save As**.

The Save As window opens.

Step 6   Click **Change** to set the recording options.

You can also set recording properties by choosing **Properties** from the Sound Recorder File menu.

The Sound Selection dialog box opens.

Step 7   From the Format drop-down menu, choose:

- CCITT u-Law if you have the G711 codec

- Option with "G729" or "G729a" in its title if you have the G729 codec

Step 8   From the Attributes drop-down menu, choose 8.000 kHz, 8 Bit, Mono 7 kb/sec.

Step 9   Click **Save As.**

The Save As dialog box opens.

Step 10   Enter a name for this format, and then click **OK**.

The Save As Dialog Box closes.

Step 11   In the Sound Selection dialog box, click **OK**.

The Sound Selection dialog box closes.

Step 12   In the Save As window, navigate to the directory of your choice, preferably a directory that you have set aside for prompts.

Step 13   Select the file name, and click **Save**.

The Save As dialog box closes.

You are now ready to add this prompt to the CRA system.

Adding a Prompt

To make prompts available to Cisco script applications, you must add them to the subdirectory in which prompts are stored.

> **Note**   Before you add a new prompt, you must create a folder to contain the .wav source files. (See Creating a Folder to Store Prompts, page 7-11.)

To add a prompt, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Prompt Management**.

The Prompt Management web page opens.

Step 2   From the Language Directory drop-down menu, choose the specific language and directory to which the prompt should be uploaded.

Step 3   To add a new prompt, click the **Add a new prompt** hyperlink.

The Prompt Upload window opens.

Step 4   In the Source File Name field, click **Browse**.

The Choose File dialog box opens.

Step 5   Navigate to the source .wav file folder, and then double-click the .wav file.

The name of the file appears in the Source File Name field.

Step 6   Click in the Destination File Name field to confirm your selection.

Step 7   Click **Upload** to upload the .wav file.

The Upload Success window opens.

Step 8   Click the **Return to Prompt Management** hyperlink.

The Prompt Management web page refreshes and the new prompt file is displayed.

Uploading a Prompt

You can replace any of the stored prompts used by Cisco script applications with a different .wav file by uploading the new .wav file. This operation replaces the previous prompt but keeps the same name for the new prompt.

To replace a prompt with a new .wav file, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Prompt Management**.

The Prompt Management web page opens.

Step 2   Click the Upload arrow for the prompt you want to upload.

The Prompt Upload window opens.

Step 3   In the Source File Name field, click **Browse**.

The Choose File dialog box opens.

Step 4   Navigate to the source .wav file folder, and then double-click the .wav file with which you want to replace the previous .wav file.

The name of the file appears in the Source File Name field.

Step 5   Click in the Destination File Name field to confirm your selection.

Step 6   Click **Upload** to upload the .wav file.

The Upload Success window opens.

Step 7   Click the **Return to Prompt Management** hyperlink.

The Prompt Management web page opens.

Adding Spoken Name Prompts

Some Cisco script applications play back the pre-recorded names of the people that callers are trying to reach, in order to allow the caller to confirm the transfer of the call.

To upload .wav files of the spoken names of users, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Spoken Name Upload**.

The Spoken Name Prompt Upload web page opens.

Step 2   In the User Id field, enter an ID number that will identify the user.

Step 3   In the Spoken Name (.wav) field, click **Browse** to navigate to the directory that contains the Spoken Name .wav file.

Step 4   Click **Upload** to upload the file.

Step 5   Repeat this process as needed to upload all spoken name .wav files.

Adding Multiple Prompts

In addition to adding .wav files individually, you can add multiple .wav files at one time.

To add multiple .wav files at one time, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **System > System Parameters**.

The System Parameters Configuration web page opens.

Step 2   Note the file path listed in the User Prompt Directory field.

Step 3   Open Windows Explorer and locate the directory that contains the .wav files for your language.

Step 4   Copy all .wav files into the directory that contains the .wav files for your language.

All your .wav files are now located in the User Prompt directory.

Install Grammars

A grammar is a specific set of all possible spoken phrases and/or Dual Tone Multi-Frequency (DTMF) digits to be recognized by CRA applications and acted upon during run time.

The CRA system uses specific grammars to recognize and respond to caller response to prompts.

The CRA system installs a set of grammars during its initial installation. You can also install your own, customized grammars.

To install your own, customized grammars, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **System > System Parameters**.

The System Parameters Configuration web page opens.

Step 2   Locate your user grammar directory contained in the User Grammar Directory field.

Step 3   Open Windows Explorer and locate the directory that contains the grammar files for your language.

Step 4   Add your customized grammar files to the directory that contains the grammar files for your language.

This grammar directory now contains all your grammar files.

You are now ready to install any customized CRA languages or to install Java files.

Install Customized CRA Languages

You can add languages to the existing set of languages that are installed with Cisco CRA.

To install customized languages, complete the following steps.

Procedure

Step 1   Open Windows Explorer and locate the CRA installation directory.

The default directory is C:\Program Files\wfavvid.

Step 2   Open the local.properties file.

The local.properties opens as a text file.

Step 3   Add additional languages to the languages.supported= line.

For example, languages.supported=en_US,en, ja_JP supports both US English and Japanese.

Do not remove existing languages that the CRA Language Installer automatically adds to the list. New languages added should be the result of adding variations to existing languages. Any totally new languages you add will lack support for internal features in the system, such as prompt generations, TTS (Text-To-Speech), and Speech Recognition.

Step 4   Save the file.

The language appears in the System Parameters page under the Default Language drop-down menu.

Install Java Files

In addition to the Java files automatically installed as part of the Cisco CRA installation process, you can install your own custom classes and Java Archive (JAR) files in order to customize the performance of your CRA system.

This section contains the following topics:

Installing Custom Classes

To install custom Java classes, complete the following steps.

Procedure

Step 1   Open Windows Explorer and locate the CRA Installation directory.

The default directory is C:\Program Files\wfavvid.

Step 2   Copy your custom Java classes into this directory.

After the CRA system loads classes and uses them once, the CRA system will not reflect changes to the classes until you restart the CRA Engine.

Your custom Java classes are now available to the CRA system.

You are now ready to install JAR files, if necessary.

Installing JAR Files

To install additional JAR files, complete the following steps.

Procedure

Step 1   Open Windows Explorer and locate the CRA Installation directory.

The default directory is C:\Program Files\wfavvid.

Step 2   Copy the JAR files into this directory.

Step 3   Locate the customengine.xml file and open the file.

Step 4   Locate the "Classpaths" tag and add the name of the file to the "Classpaths" tag.

Your JAR files are now available to the CRA system.

Add a Cisco Script Application

Now that you have completed the pre-application tasks by uploading your scripts, prompts, grammars, languages, and custom classes, you need to create a new application.

To add a new Cisco script application, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Application Configuration web page opens.)

Step 2 Click the **Add a New Application** hyperlink.

The Add a New Application web page opens.

Step 3 In the Application Type drop-down menu, choose Cisco Script Application, and then click **Next**.

The Cisco Script Application web page opens.

Step 4 In the Name field, enter the name of the script.

Step 5 Press the **Tab** key to automatically populate the Description field.

Step 6 In the ID field, accept the automatically generated ID, or enter a unique ID.

The Historical Reporting feature uses this ID to identify this application.

Step 7 In the Maximum Number of Sessions field, enter the maximum number of simultaneous sessions that the application can handle.

Step 8 From the Script drop-down menu, choose the script to run the application.

If the script contains parameters, the parameters display below the Script drop-down menu. Each parameter has a check box, which enables you to override the default value for that parameter. If you want to override the value, check the check box for that parameter.

Step 9 From the Default Script drop-down menu, accept **System Default**.

The default script is executed when an error occurs with the configured application script.

Step 10   Click **Add**.

The following message appears:

`The operation has been executed successfully.`

The Cisco Script Application web page is refreshed, and the information you entered appears.

Depending on your script selection, the web page may provide additional fields and drop-down menu options when refreshed.

You are now ready to configure a trigger for this application.

After you add an application, you can modify the application by clicking any of the application's name or other information in the Application Configuration page. The page for that application opens, enabling you to modify the application's settings.

Add an Application Trigger

Triggers are specified signals that invoke application scripts in response to incoming contacts. The CRA system uses JTAPI triggers to trigger responses to telephone calls and HTTP triggers to respond to HTTP requests.

After adding a new Cisco script application, you need to add one or more triggers so that the application can respond to JTAPI calls and/or HTTP requests.

Note   Before you add application triggers, you must configure route points in Cisco CallManager. For more information, see the "Add CTI Route Points" section on page 2-6).

You can use either of two methods to add a trigger to an application: Add the trigger from the Cisco Script Application web page or add the trigger from the JTAPI or HTTP subsystem.

This section contains the following procedures:

- Adding a JTAPI Trigger, page 7-22
- Adding an HTTP Trigger, page 7-25

Adding a JTAPI Trigger

You must add JTAPI triggers to invoke Cisco script applications in response to incoming contacts.

A JTAPI trigger responds to calls that arrive on a specific route point by selecting telephony and media resources to serve the call and invoking an application script to handle the call.

This section contains the following procedures:

- Add a JTAPI Trigger from the Cisco Script Application Web Page, page 7-22
- Add a JTAPI Trigger from the JTAPI Subsystem, page 7-23

Add a JTAPI Trigger from the Cisco Script Application Web Page

To add a JTAPI trigger directly from the Cisco Script Application web page, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Applications Configuration web page opens.

Step 2   In the display list, click the Cisco script application for which you want to add the JTAPI trigger.

The Cisco Script Application web page opens.

Step 3   On the Cisco Script Application navigation bar, click the **Add New Trigger** hyperlink.

The Add a New Trigger window opens.

Step 4   From the Trigger Type drop-down menu, choose **JTAPI**.

Step 5   Click **Next**.

The JTAPI Trigger Configuration window opens.

Step 6   From the CTI Route Point Directory Number drop-down menu, choose the CTI (Computer Telephony Interface) route point number that you configured in Cisco CallManager.

For information on how to create a Cisco CTI route point, see the "Add CTI Route Points" section on page 2-6.

Step 7   From the Language drop-down menu, choose the appropriate default language, or accept the system default language.

Step 8   In the Maximum Number of Sessions field, enter the maximum number of simultaneous sessions that the application can handle.

Step 9   In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait for all the required resources to process a call and to invoke the application before rejecting a call.

Step 10   From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 11   From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group.

You can choose **No Group** if the application being triggered by this trigger does not require a media resource.

Step 12   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 13   Click **Add**.

The Application Configuration web page opens, and the JTAPI route point appears on the Application Configuration navigation bar.

Add a JTAPI Trigger from the JTAPI Subsystem

To add a JTAPI trigger to an application from the JTAPI subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems> JTAPI**.

The JTAPI Configuration web page opens.

Step 2   On the JTAPI Configuration navigation bar, click the **JTAPI Triggers** hyperlink.

The first JTAPI Trigger Configuration web page opens.

Step 3   Click the **Add a New JTAPI Trigger** hyperlink.

The second JTAPI Trigger Configuration web page opens.

Step 4   From the CTI Route Point Directory Number drop-down menu, choose the CTI route point number that you configured in Cisco CallManager.

For information on how to create a Cisco CTI route point, see "Add CTI Route Points" section on page 2-6.

Step 5   From the Language drop-down menu, choose the appropriate default language, or accept the system default language.

Step 6   From the Application Name drop-down menu, choose the appropriate application to associate with this trigger.

Step 7   In the Maximum Number of Sessions field, enter the maximum number of sessions.

This value is the maximum number of simultaneously running applications that can be triggered by this particular trigger.

Step 8   In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait for all the required resources to process that call and for the right to invoke the application before rejecting a call.

Step 9   From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 10   From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group or none.

You can choose **No Group** if the application being triggered by this trigger does not require media resources.

Step 11   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 12   Click **Add**.

The first JTAPI Trigger Configuration web page opens, showing the new JTAPI trigger.

Adding an HTTP Trigger

A Cisco script application can be used to handle HTTP requests when the CRA system is provisioned with an HTTP trigger.

An HTTP trigger is the relative URL a user enters into the client browser to start the application. You can upload either eXtensible Style Language Transformation (XSLT) templates or Java Server Pages (JSP) templates to serve as your HTTP trigger.

The following path is an example of an HTTP-triggered request (using the HTTP trigger name "/hello"):

```
http://www.appserver.acme.com:8080/hello
```

In this example, the URL starts the application with the HTTP trigger "/hello" on a web server running on port 8080 with the host name www.appserver.acme.com.

You can add the HTTP trigger from the Cisco Script Application web page or add the trigger from the HTTP subsystem.

This section contains the following procedures:

- Add an HTTP Trigger from the Cisco Script Application Web Page, page 7-25
- Add an HTTP Trigger from the HTTP Subsystem, page 7-27

Add an HTTP Trigger from the Cisco Script Application Web Page

To add an HTTP trigger directly from the Cisco Script Application web page, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Applications Configuration web page opens.

Step 2   In the display list of the Application Configuration web page, click the Cisco script application for which you want to add the HTTP trigger.

The Cisco Script Application web page opens.

Step 3   On the Cisco Script Application navigation bar, click the **Add New Trigger** hyperlink.

The Add a New Trigger web page opens.

Step 4   From the **Trigger Type** drop-down menu, choose HTTP, and then click **Next**.

The HTTP Trigger Configuration window opens.

Step 5   In the **URL** field, enter the relative URL.

For example:

```
http://www.appserver.acme.com:8080/hello
```

Step 6   From the Language drop-down menu, choose a default language, or choose **Keep Browser Settings** to use the browser default language.

Step 7   In the Maximum Number of Sessions field, enter the maximum number of sessions that can be served by the HTTP subsystem for this trigger.

Step 8   In the Idle Timeout (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

Step 9   In the Enabled field, click the **Yes** radio button to activate the trigger, or click the **No** radio button if, for example, you want to disable the trigger for system repair.

If you disable the trigger, the user receives an error message when browsing to the defined trigger URL.

Step 10   Click **Add**.

The Cisco Script Application web page opens, and the URL of the HTTP trigger appears on the Cisco Script Application navigation bar.

Step 11   To test the trigger, enter the URL you just configured in the address bar of your browser.

For example,

```
http://www.appserver.acme.com:8080/hello
```

The browser should display "hello".

Add an HTTP Trigger from the HTTP Subsystem

To configure a HTTP trigger from the HTTP subsystem, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Subsystems > HTTP**.

The first HTTP Trigger Configuration window opens.

Step 2   Click the **Add a New HTTP Triggers** hyperlink.

The second HTTP Trigger Configuration window opens.

Step 3   In the **URL** field, enter the relative URL.

For example:

```
http://www.appserver.acme.com:8080/hello
```

Step 4   From the Language drop-down menu, choose a default language, or choose **Keep Browser Settings** to use the browser default language.

Step 5   In the Maximum Number of Sessions field, enter the maximum number of sessions that can be served by the HTTP subsystem for this trigger.

Step 6   In the Idle Timeout (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

Step 7   In the Enabled field, click the **Yes** radio button to activate the trigger, or click the **No** radio button if, for example, you want to disable the trigger for system repair.

If you disable the trigger, the user receives an error message when browsing to the defined trigger URL.

Step 8   Click **Add**.

The Cisco Script Application appears, and the URL of the HTTP trigger appears on the Cisco Script Application navigation bar.

Step 9   To test the trigger, enter the URL you just configured in the address bar of your browser.

For example,

```
http://www.appserver.acme.com:8080/hello
```

The browser should display "hello".

You are now ready to configure additional CRA applications. (See Chapter 8, "Configuring Additional CRA Applications."

Configuring Additional CRA Applications

Complete the following tasks before configuring additional CRA applications:

- Configure your Cisco CallManager to communicate with the Cisco CRA server (see Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

- Set up your IP telephony directory (see Chapter 3, "Setting Up the Cisco IP Telephony Directory.")

- Provision your telephony and media resources (see Chapter 4, "Provisioning Telephony and Media.")

- Provision your Integrated Contact Distribution (ICD) subsystem, if necessary (see Chapter 5, "Provisioning Cisco IP ICD.").

- Provision any additional subsystems your CRA applications will require (see Chapter 6, "Provisioning Additional Subsystems.")

- Configure your Cisco script applications (see Chapter 7, "Configuring Cisco Script Applications."

You must now configure any additional CRA applications your CRA system will require.

Note   Before you configure applications, you must follow the procedures in Chapter 4 and Chapter 6 to provision the system to handle Java Telephony Application Programming Interface (JTAPI) calls and HTTP requests. (For more information, please see the "Provision the JTAPI Subsystem" section on page 4-3 and the "Provision the HTTP Subsystem" section on page 6-7.)

The Cisco CRA system uses applications to interact with contacts and perform a wide variety of functions. (For information on configuring Cisco script applications, see Chapter 7, "Configuring Cisco Script Applications.") The CRA system also uses four additional types of applications.

To configure additional CRA applications, you will need to perform the following tasks:

1. Configure the Busy application. This application, which comes with each CRA package, plays a busy signal.

2. Configure the Ring-No-Answer (RNA) application. This application, which comes with each CRA package, plays a ring tone.

If you are using Cisco ICM, you will also need to perform one or both of the following tasks:

- Configure ICM post-routing applications. These applications are used by the Cisco IP IVR (Interactive Voice Response) system to receive calls directly from Cisco CallManager, which sends the call to the post-routing route point on the Cisco CRA system.

- Configure ICM translation-routing applications. These applications use the CRA server as a queue point for Cisco IPCC (IP Call Center), so that Cisco ICM can route calls to the CRA server.

Note   If you are not using Cisco ICM, you will not need to configure ICM post-routing and ICM translation-routing applications.

You must be logged into the CRA Administration web interface to perform these tasks.

This chapter introduces these four additional CRA application types and explains how to configure them. It includes the following procedures:

Configure the Busy Application

The Cisco Busy application comes with each CRA package.

The Cisco Busy application returns a busy signal when a call reaches a CTI (Computer Telephony Interface) route point and the extension is busy.

Note   Before you can configure the Busy application, you must configure CTI route points. (For more information on how to configure route points, see the "Add CTI Route Points" section on page 2-6.)

To configure the Busy application, you will need to perform the following tasks:

1. Add the Busy application. You need to add the script that provides the busy signal to make it available to CRA applications.

2. Add a Java Telephony Applications Programming Interface (JTAPI) trigger to the Busy application. The Busy application is activated when it is triggered by a JTAPI trigger. (The Busy application does not support HTTP triggers.)

To configure the Cisco CRA server with the Busy application, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Application Configuration web page opens.

Step 2   Click the **Add a New Application** hyperlink.

The Add a New Application web page opens.

Step 3   From the Application Type drop-down menu, choose **Busy**, and then click **Next**.

The Busy web page opens.

Step 4   In the Name field, enter the name of the script.

Step 5   Press the **Tab** key to automatically populate the Description field.

Step 6   In the ID field, accept the default ID, or enter a unique ID.

Step 7   In the Maximum Number of Sessions field, enter the maximum number of simultaneous sessions that the application can handle.

Step 8   In the Enabled field, accept the default **Yes** radio button.

Step 9   Click **Add**.

The Busy web page refreshes. The **Add New Trigger** hyperlink appears on the Busy navigation bar, and a dialog box opens with the following message:

```
The operation has been executed successfully
```

Step 10   Click **OK** to close the dialog box.

Step 11   Click the **Add New Trigger** hyperlink.

The **Add a New Trigger** window opens.

Step 12   From the Trigger Type drop-down menu, choose **JTAPI**, and then click **Next**.

The JTAPI Trigger Configuration window opens.

Step 13   From the CTI Route Point Directory Number drop-down menu, choose the CTI route point number that you configured in Cisco CallManager.

Step 14   From the Language drop-down menu, choose the appropriate language or accept the default language.

This choice is useful in the Busy application only if the busy tones have been re-recorded for a specific country.

The Application Name field is automatically populated with the Application Name.

Step 15   In the Maximum Number of Sessions field, enter the maximum number of sessions that the JTAPI subsystem can serve for this trigger.

Step 16   In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait before rejecting a call.

Step 17   In the Enabled field, accept the default **Yes** radio button.

Step 18   From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 19   From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group.

You must select a CMT (Cisco Media Termination) group for this application to work because the application must simulate a busy tone by playing prompts. If you do not select a CMT group, the application will not function correctly.

Step 20   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 21   Click **Add**.

The Busy web page opens, displaying the configured route point on the Busy navigation bar.

You are now ready to configure the Ring-No-Answer Application.

Configure the Ring-No-Answer Application

The Cisco Ring-No-Answer application comes with each CRA package.

The Cisco Ring-No-Answer application returns a ring tone signal when a call reaches a CTI route point.

Note   Before you can configure the Ring-No-Answer application, you must configure CTI route points. (For more information on how to configure route points, see "Add CTI Route Points" section on page 2-6.)

To configure the Ring-No-Answer application, you will need to perform the following tasks:

1. Add the Ring-No-Answer application. You need to add the script that provides the ring tone make it available to CRA applications.

2. Add a JTAPI trigger to the Ring-No-Answer application. The Ring-No-Answer application is activated when it is triggered by a JTAPI trigger.

To configure the Cisco CRA server with the Ring-No-Answer application, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Application Configuration web page opens.

Step 2 Click the **Add a New Application** hyperlink.

The Add a New Application web page opens.

Step 3 From the Application Type drop-down menu, choose **Cisco ICM Ring-No-Answer**, and then click **Next**.

The Ring-No-Answer web page opens.

Step 4 In the Name field, enter the name of the script.

Step 5 Press the **Tab** key to automatically populate the Description field.

Step 6 In the ID field, accept the default ID, or enter a unique ID.

Step 7 In the Maximum Number of Sessions field, enter the maximum number of simultaneous sessions that the application can handle.

Step 8 In the Enabled field, accept the **Yes** default radio button.

Step 9 Click **Add**.

The Ring-No-Answer web page refreshes. The **Add New Trigger** hyperlink appears on the Ring-No-Answer navigation bar, and a dialog box opens with the following message:

```
The operation has been executed successfully
```

Step 10 Click **OK** to close the dialog box.

Step 11 On the Ring-No-Answer navigation bar, click the **Add New Trigger** hyperlink.

The **Add a New Trigger** window opens.

Step 12 From the Trigger Type drop-down menu, choose **JTAPI**, and then click **Next**.

The JTAPI Trigger Configuration window opens.

Step 13 From the CTI Route Point Directory Number drop-down menu, choose the CTI route point number that you configured in Cisco CallManager.

Step 14   From the Language drop-down menu, choose the appropriate language, or accept the default language.

Since CRA system simulates the RNA tone, changing the language is useful only if this particular call requires a different type of ringing tone that has been re-recorded and installed in a system prompt directory corresponding to the language selected.

The Application Name field is automatically populated with the application name.

Step 15   In the Maximum Number of Sessions field, enter the maximum number of sessions that the application will be able to handle simultaneously.

Step 16   In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait before rejecting a call.

Step 17   In the Enabled field, accept the default radio button **Yes**.

Step 18   From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 19   From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group.

You must select a CMT group for this application to work because the application must simulate the RNA tone by playing prompts. If you do not select a CMT group, the application will not function correctly.

Step 20   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 21   Click **Add**.

The the Ring-No-Answer web page opens, and the route point is displayed on the Ring-No-Answer navigation bar.

Unless you are using Cisco ICM, you are now ready to configure the Historical Reporting databases. (See Managing the Cisco CRA Historical Report Databases, page 9-1.)

If you are using Cisco ICM, you are now ready to configure Cisco ICM post-routing or translation-routing applications.

Configure a Cisco ICM Post-Routing Application

Cisco Intelligent Contact Management (ICM) post-routing applications use the CRA server as a queue point for Cisco IPCC. In Cisco ICM post-routing, the Cisco IP IVR system receives calls directly from Cisco CallManager, which sends the call to the post-routing route point on the CRA system.

If you configure this route point to run an initial application, such as an application to welcome the caller and collect an account number, the CRA system notifies the Cisco ICM about the call, and then waits for further instructions. If you do not configure an initial script, the CRA system informs the Cisco ICM about the call, but takes no other action.

After notification, the Cisco ICM system runs an ICM script, which can be composed of many different call-handling steps, including three commands that can be sent to the CRA system:

- **Connect**—This request is automatically sent by the Cisco ICM whenever an agent is available and the call can be connected to that agent.

- **Release**—This request releases the call.

- **Run VRU Script**—This request runs the VRU (Voice Response Unit) script.

> **Note** Before you add a Cisco ICM application, you must configure route points (see the "Add CTI Route Points" section on page 2-6), and configure Nuance Automatic Speech Recognition (ASR) dialog groups (see the "Provision the Nuance ASR Subsystem" section on page 4-10.)
> Before you can configure a Cisco ICM post-routing application, you must first upload any VRU scripts that the application will need. (For more information, see the "Provision the ICM Subsystem" section on page 6-3.)

To configure a Cisco ICM post-routing application, you will need to perform the following tasks:

1. Add a Cisco ICM post-routing application. In addition to configuring general information such as name and ID, you must specify the script on which the ICM post-routing application is based.

2. Add a JTAPI trigger to the ICM post-routing application. The ICM post-routing application is invoked by a JTAPI trigger. (The ICM post-routing application does not support HTTP triggers.)

To configure the Cisco CRA server with the post-routing application and to add a JTAPI trigger, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Application Configuration web page opens.

Step 2   Click the **Add a New Application** hyperlink.

The Add a New Application web page opens.

Step 3   From the **Application Type** drop-down menu, choose **Cisco ICM Post-Routing**.

The Cisco ICM Post-Routing web page appears.

Step 4   In the **Name** field, enter the name of the script.

Step 5   Press the **Tab** key to automatically populate the **Description** field.

Step 6   In the **ID** field, accept the ID or enter a unique ID.

This ID is the service identifier that will be reported with the call back to Cisco ICM.

Step 7   In the Maximum Number of Sessions field, enter the maximum number of sessions that the application can to handle simultaneously.

Step 8   In the Enabled field, accept the default radio button **Yes**.

Step 9   In the Timeout (in secs) field, enter a value (in seconds).

This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

Step 10   From the Initial Script drop-down menu, choose the script to run when the CRA receives a call.

This script can be used to acquire initial digits from the caller and report the information to Cisco ICM as part of the notification of the incoming call. This capability allows Cisco ICM to correctly choose a Cisco ICM script to serve the call.

Step 11   From the Default Script drop-down menu, choose the script the will be run if a system error occurs, or if requested by Cisco ICM, to route the call to the default treatment.

Step 12 Click **Add**.

The Cisco ICM Post-Routing web page refreshes. The **Add New Trigger** hyperlink appears on the Cisco ICM Post-Routing navigation bar, and a dialog box opens with the following message:

```
The operation has been executed successfully
```

Step 13 Click **OK** to close the dialog box.

Step 14 On the Cisco ICM Post-Routing navigation bar, click the **Add New Trigger** hyperlink.

The **Add a New Trigger** web page opens.

Step 15 From the Trigger Type drop-down menu, choose **JTAPI**, and then click **Next**.

The JTAPI Trigger Configuration web page opens.

Step 16 From the CTI Route Point Directory Number drop-down menu, choose the CTI route point number that you configured in the Cisco CallManager.

Step 17 From the Language drop-down menu, choose the appropriate language, or accept the system default language.

The Application Name field is automatically populated with the Application Name.

Step 18 In the Maximum Number of Sessions field, enter the maximum number of sessions that can be triggered by this trigger simultaneously.

Step 19 In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait before rejecting a call.

Step 20 In the Enabled field, accept the default radio button **Yes**.

Step 21 From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 22 From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group, or none.

Step 23   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 24   Click **Add**.

The route point appears in the Cisco ICM Post-Routing web page.

Configure a Cisco ICM Translation-Routing Application

You must configure Cisco ICM translation-routing applications when the CRA server is used as a queue point for a Cisco IPCC solution (Cisco IP Queue Manager) in which calls are expected to be routed by the Cisco ICM to the CRA server.

The call attributes will be reported as part of a configured translation-route on the Cisco ICM.

Note   Before you can configure a Cisco ICM translation-routing application, you must first upload any VRU scripts that the application will need. (For more information, see the "Provision the ICM Subsystem" section on page 6-3.)

To configure the ICM translation-routing application, you will need to perform the following tasks:

1.   Add a Cisco ICM translation-routing application.

In addition to configuring general information such as name and ID, you must specify the script on which the ICM translation-routing application is based.

2.   Add a JTAPI trigger to the ICM translation-routing application.

The ICM translation-routing application is invoked by a JTAPI trigger. (The ICM translation-routing application does not support HTTP triggers.)

To configure the Cisco CRA server with a Cisco ICM translation-routing application and to add a JTAPI trigger, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Applications > Configure Applications**.

The Application Configuration web page opens.

Step 2   Click the **Add a New Application** hyperlink.

The Add a New Application web page opens.

Step 3   From the Application Type drop-down menu, choose **Cisco ICM Translation-Routing**.

The Cisco ICM Translation-Routing web page opens.

Step 4   In the Name field, enter the name of the script.

Step 5   Press the **Tab** key to automatically populate the Description field.

Step 6   In the ID field, accept the ID, or enter a unique ID.

This field corresponds to the service identifier of the call reported to the Cisco ICM and configured in the Cisco ICM translation route.

Step 7   In the Maximum Number of Sessions field, enter the maximum number of sessions that the application will be able to handle simultaneously.

Step 8   In the Enabled field, accept the default radio button **Yes**.

Step 9   In the Timeout (in secs) field, enter a value (in seconds).

This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

Step 10 From the Default Script drop-down menu, choose the script that will be run if a system error occurs, or if instructed by the Cisco ICM to route to the default treatment.

Step 11 Click **Add**.

The Cisco ICM Post-Routing web page refreshes. The **Add New Trigger** hyperlink appears on the Cisco ICM Post-Routing navigation bar, and a dialog box appears with the following message:

```
The operation has been executed successfully
```

Step 12 Click **OK** to close the dialog box.

Step 13   On the Cisco ICM Post-Routing navigation bar, click the **Add New Trigger** hyperlink.

The **Add a New Trigger** web page opens.

Step 14   From the Trigger Type drop-down menu, choose **JTAPI**, and then click **Next**.

The JTAPI Trigger Configuration web page opens.

Step 15   From the CTI Route Point Directory Number drop-down menu, choose the CTI route point number that you configured in the Cisco CallManager.

Step 16   From the Language drop-down menu, choose the appropriate language, or accept the default language.

The Application Name field is automatically populated with the Application Name.

Step 17   In the Maximum Number of Sessions field, enter the maximum number of sessions that can be simultaneously triggered by this trigger.

Step 18   In the Idle Time-out (in ms) field, enter a maximum value (in milliseconds).

This value is the maximum amount of time that the system will wait before rejecting a call.

Step 19   In the Enabled field, accept the default radio button **Yes**.

Step 20   From the Call Control Group drop-down menu, choose the appropriate call control group.

Step 21   From the Primary Dialog Group drop-down menu, choose the appropriate primary dialog group, or none.

Step 22   From the Secondary Dialog Group drop-down menu, choose the appropriate secondary dialog group, or none.

Step 23   Click **Add**.

The route point appears in the Cisco ICM Translation-Routing web page.

You are now ready to set up the Historical Reporting databases. (See Managing the Cisco CRA Historical Report Databases, page 9-1.)

Configure a Cisco ICM Translation-Routing Application

Managing the Cisco CRA Historical Report Databases

The Cisco CRA system historical databases can reside either on the CRA server machine or on the Historical Report Database server machine.

Managing the CRA Historical Report databases involves:

- Configuring maximum number of client and scheduler connections to the historical databases. If the Historical Report Database server is being used to store historical reporting data, the IP address of the database server must also be configured.

- Configuring users for historical reports.

- Purging historical data when the size of the databases approaches maximum capacity.

- Synchronizing data on the CRA server databases and Historical Report Database Server database, if the Historical Report Database server is being used to store historical reporting data.

- Importing historical data from data files. These data files are generated if the historical database is down and the number of new historical records exceeds the cache.

You must be logged in to the CRA Administration in order to manage the CRA historical reports database.

This chapter contains the following topics:

About the CRA System Databases

This section describes the CRA system databases, including:

Historical Database Names

When you install the Cisco CRA system, the installation process creates two databases that the system uses to store data for historical reports. These databases are described in Table 9-1.

Table 9-1   CRA System Historical Databases

Database Name	Description
Db_cra	Contains most information for historical reports, including information about resource groups, skills, and resources.
Db_cra_ccdr	Contains information about each call that the system processes.

If you install the Historical Report Database server, the installation process creates these databases on the Historical Report Database server. The CRA system writes historical data directly to the Historical Report Database server databases and only writes historical data to the local databases if the connection to the Historical Report Database server cannot be established.

Historical Database Sizing

You can configure the CRA system to store historical data in local databases or in databases on the Historical Report Database server, which is installed on a separate machine from the CRA server. You can use the Historical Report Databases server regardless of whether you install the CRA Engine on the same machine as Cisco CallManager or on its own machine.

Microsoft SQL Desktop Edition (MSDE) databases are used to store historical data on the CRA server if historical data is stored locally.

If you install the CRA Engine on the same server as Cisco CallManager and historical data is stored locally, the CRA system uses the MS SQL Server databases on that server to store historical data.

On the Historical Report Database server (if it is installed), you can use either MS SQL Server databases or MSDE databases. MSDE supports up to 15 concurrent historical reporting clients. If you want to support more historical reporting clients, use MS SQL Server.

The CRA system determines the size of the historical reports databases, as described in Table 9-2.

Table 9-2   Database Sizing

Database Type	Database Size
MSDE database	If free disk space on the server is greater than 8 GB, the maximum size of each database is 2 GB. If free disk space on the server is less than 8 GB, the maximum size of each database is one-fourth of the free disk space. For example, if free disk space on the server is 4 GB, the size of each database will be 1 GB
MS SQL Server database	The default size of each database is 256 MB. ⚠️ **Caution** If you change the default size of an MS SQL database, make sure that the space allocated and the maximum file size are the same. If these values are not the same, purging will not function properly.

The CRA system limits the number of records in a report to 500,000 records from CCDR (Contact Call Detail Record) by all stored procedures.

To change or disable this limit, run the setHistMaxRecCount.bat file from the wfavvid install directory on the server used to store historical data, with the following usage: setHistMaxRecCount "*dbUserName*" and "*dbPassword*" MaxRecordCount. (Make sure that you enclose *dbUserName* and *dbPassword in* double quotes [" "].)

The following are examples of change and disable limit syntax:

- Change limit—setHistMaxRecCount "sa" "" 400000.
- Disable limit—setHistMaxRecCount "sa" "" 0.

✎

Note   If you increase or disable the records limit, you will affect your CRA system performance.

Configuring the Database Server

You can configure the maximum number of client and reporting sessions that can access the historical reporting databases.

If you are using the Historical Report Database server to store historical data, you also need to specify the IP address of the Historical Report Database server.

> **Note** If you specify the IP address of the Historical Report Database server, you cannot change the IP address back to the local CRA server.

Before configuring the database server, you must stop the CRA Engine. Restart the CRA Engine after you have updated the configuration for the changes to take effect.

To configure the database server, complete the following steps.,

Procedure

Step 1 From the CRA Administration menu bar, choose **System > Engine**.

The Engine web page opens, displaying the Engine Status page.

Step 2 Click **Stop Engine**.

Step 3 From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens, displaying the Database Server Configuration area.

Step 4 If you have installed the Historical Report Database Server, enter the IP address of the server on which the historical database is installed in the Historical Report Database Server field.

The default value is the local IP address of the CRA server.

Step 5 Enter the maximum number of historical reporting client connections and scheduler connections in the Maximum DB Connections for Report Client Sessions field.

Step 6 Click **Update**.

Step 7 From the CRA Administration menu bar, choose **System > Engine**.

The Engine web page opens, displaying the Engine Status page.

Step 8 Click **Start Engine**. The configuration changes take effect.

Synchronizing Data on the Local and Historical Report Databases

If the Historical Report Database server is installed, the CRA server records data as follows:

- Historical data is written directly to the Historical Database server.

- ICD configuration data is written directly to the local CRA server. A copy of the ICD configuration data is stored on the Historical Report Database server. Updates to configuration data on the local server trigger updates to the Historical Report Database server.

If the connection between the CRA server and the Historical Report Database server cannot be established (for example, if the network connection goes down), the CRA server writes historical data to the local databases and flags new or changed ICD configuration database records to be synchronized when the connection is reestablished.

When the connection between the CRA server and Historical Report Database server is reestablished, the data on the Historical Report Database server must be synchronized with the data on the CRA server.

Tip If a Historical Reports Database Server is set up and you have restored backed-up data on the Cisco CRA Server but not on the Historical Reports Database Server, MIVR logs show that historical records fail because of primary key conflicts. (Both servers should always be backed up at the same time.) To workaround this problem, restore the backed-up data to the Historical Reports Database Server manually, as described in the "Synchronizing Data Manually (Tools Menu method)" section on page 9-8 or "Synchronizing Data Manually (Text Editor method)" section on page 9-9.

You can enable and schedule automatic synchronization of the data on the CRA server databases and Historical Report Database server databases. You can also synchronize the data manually at any time.

Note   The historical records are removed from the CRA server after the data has been updated on the Historical Report Database server.

This section describes:

Synchronizing Data Automatically

Automatic historical and ICD configuration data synchronization ensures proper system functioning.

You can enable automatic synchronization if it is currently disabled. If the connection between the CRA server and Historical Reports Database server fails and is reestablished, the Historical Reports Database server checks whether any data is out of sync between the CRA server local databases and the Historical Reports Database server databases. If data is out of sync, the Historical Reports Database server automatically updates the data according to the schedule that you specify.

To configure automatic historical and configuration data synchronization, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens, displaying the Database Server Configuration area.

Step 2   Look in the **Database Server Status** area to ensure that the Historical Reports Database server status is "Available". You can configure automatic synchronization only if the status is Available.

Step 3 Click the **Synchronize Data** hyperlink on the Historical Reporting Configuration navigation bar**.**

Step 4 Check the Enable Historical Data Synchronizer check box to enable automatic historical data synchronization.

Step 5 Select a time of day at which to synchronize the historical data from the drop-down menu.

Because historical data synchronization can be a lengthy process, especially if you are upgrading from a previous version of Cisco CRA, synchronize data at an off-peak time or a time at which the system is not receiving calls.

Step 6 Check the Enable Configuration Data Synchronizer check box to enable automatic configuration data synchronization.

Step 7 Select the interval, in minutes, at which to synchronize the configuration data.

The default value is **5** minutes.

Step 8 Click **Update** to apply the synchronization schedule changes.

Synchronizing Data Manually (Tools Menu method)

You can manually synchronize the historical and configuration data in the CRA server local databases and Historical Reports Database server databases at any time using the CRA Administration's Tools menu. This action will not affect the automatic synchronization schedule. However, you cannot manually synchronize data while the automatic synchronization is executing.

To synchronize historical and configuration data manually using the Tools menu, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens, displaying the Database Server Configuration area.

Step 2 Click the **Synchronize Data** hyperlink on the Historical Reporting Configuration navigation bar**.**

The Synchronize Data area opens.

Step 3   Check that atheistically Data Synchronizer Status and Configuration Data Synchronizer Status, listed in the Synchronize Now area, are both "Not Executing". If either are executing, you cannot manually synchronize data. You can only synchronize data manually when neither are executing.

Step 4   Click **Synchronize Now**.

If automatic synchronization currently is executing, a message appears instructing you to manually synchronize at another time. Otherwise, the historical and configuration data is synchronized.

Synchronizing Data Manually (Text Editor method)

To synchronize historical and configuration data manually using a text editor to modify the wfengine.properties and application.properties files, complete the following steps.

Procedure

Step 1   Use a text editor to open the following file:

C:\program files\WFAVVID\ wfengine.properties.

(The file might be in another folder if you did not install Cisco CRA in the default folder.)

Step 2   Add 1000 to the value of the following property:

com.cisco.wfframework.engine.APPLICATION_TASKID_BLOCK

Step 3   Save the wfengine.properties file.

Step 4   Use a text editor to open the following file:

C:\program files\WFAVVID\ application.properties.

(The file might be in another folder if you did not install Cisco CRA in the default folder.)

Step 5   Add 1000 to the value of the following property:

com.cisco.session.id.block

Step 6   Save the application.properties file.

Configuring Users for Historical Reporting

You can enable users configured on the Cisco CallManager to use installed CRA historical reporting packages.

To configure users for historical reporting, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens, displaying the Database Server Configuration area.

Step 2   Click the **User Configuration** hyperlink on the Historical Reporting Configuration navigation bar.

The User Configuration area opens, listing a maximum of 75 Cisco CallManager users.

Step 3   Choose the user for which you want to configure historical reporting by either:

- Entering search criteria (such as a user name) in the Enter Search Criteria text field and then choosing the appropriate user from the drop-down list. If more than 75 users are configured on Cisco CallManager, you can use search to find user who are not displayed.

- Choosing the user from the drop-down list.

Step 4   Click **Next**.

The User configuration for user area opens.

Step 5   In the Installed Reporting Packages list, choose the reporting package for which you want to configure this user, and click >.

Step 6   If you want to remove reporting packages from this user, choose the reporting package that you want to remove in the Selected Reporting Packages list, and click < .

Step 7   Click **Update** to apply the changes.

The User Configuration area opens.

Step 8   Repeat steps 3 through 7 to configure additional users.

Purging Historical Data

As the Cisco CRA Engine runs, it collects information about the status and performance of the CRA system. Historical information is stored in databases that can then be accessed to provide reports. (Refer to the *Cisco Customer Response Applications Historical Reports User Guide* for more information about Cisco CRA Historical Reports.)

When either of the historical reports databases approaches its maximum size, some or all of the data in it must be removed. Removing data from a database is called *purging*.

When the system purges data, it removes historical data from both the Db_cra_ccdr database and Db_cra database.

When the system purges data from the historical reports databases, it determines what information to purge based on the number of months you specify and on the current date. For example, if you instruct the system to purge data older than 12 months, a purge on January 15 will purge data older than January 15 of the previous year.

Note   When you purge data, you permanently delete it. If you want to keep data that will be purged, back up the databases.

Cisco CRA Administration provides the following features for purging historical reports databases:

- Daily comparison of the size of the databases to a user-specified maximum size
- User-specified time at which the system purges data
- Automatic purging of databases when they exceed the user-specified maximum sizes
- Automatic purging of databases based on user-specified parameters

- Manual purging of databases
- Automatic e-mail notification of purging activities
- Automatic SNMP (Simple Network Management Protocol) traps and Syslog messages describing purging activities

This section describes:

Configuring Automatic Purging

The CRA Engine performs automatic purging each day at a preset time. To help keep your system running most efficiently, Cisco recommends that you schedule automatic purging to run when your system is least busy. By default, daily purges are scheduled to run at 4:00 a.m. (0400), but you can change this time.

The system bases its purging activities on a variety of parameters. You can change the default value for any parameter as needed.

A log file, PurgeProcess.log, stores information about the automatic purging activities that the system performs. The PurgeProcess.log file has a maximum size of 2 MB. When this file reaches its maximum size, the system copies it to a backup file named PurgeProcess.bak. The system maintains one such backup file. Each time the PurgeProcess.log file reaches 2 MB in size, the system moves that information to the existing backup file, overwriting the information in the existing backup file. This log file is stored on the CRA server in the *<CRAinstallationDirectory>*\wfavvid\log\Purge_Sch directory. (By default, the system installs in the Program Files directory.) You can view this log file by opening the file in a text editor.

This section contains the following procedures:

Managing the Purging Scheduler Service

The Cisco Purging Scheduler Service must be running on the CRA server for automatic purging to occur. By default, this service is always running. If you turn off this service, make sure to monitor the sizes of the databases and purge them manually as needed.

If you change the server system clock, you must stop and restart the Cisco Purging Scheduler Service for automatic purging to occur at the correct time.

To verify that the Cisco Purging Scheduler Service is running, and to restart it or stop it, if necessary, perform the following steps:

To start or stop the Purge Scheduler Service, complete the following steps.

Procedure

Step 1   From the Windows desktop, choose **Start > Settings > Control Panel**.

The Control Panel window opens.

Step 2   Double-click **Administrative Tools**.

The Administrative Tools window opens.

Step 3   Double-click **Services**.

The Services window opens.

Step 4   Look at the Status field of the Cisco Purge Scheduler Service. If this field displays "Started," the Purging Scheduler Service is running. If this field is blank, the Purge Scheduler Service is not running.

- To start the Purging Scheduler Service, right-click **Cisco Purging Scheduler Service** in the Services Window, and then choose **Start** from the Services menu.

- To stop the Purging Scheduler Service, right-click **Cisco Purging Scheduler Service** in the Services Window, and then choose **Stop** from the Services menu.

Setting the Daily Purge Schedule

You can change the time of day that the system assesses the need to purge data and the age of data to purge.

To set the purge schedule, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens, displaying the User Configuration area.

Step 2   Click the **Purge Schedule** hyperlink on the Historical Reporting Configuration navigation bar**.**

The Purge Schedule area opens.

Step 3   From the Daily Purge At drop-down menu, choose a time of day at which the system determines if purging is necessary.

Step 4   From the Purge Data Older Than *N* Months drop-down menu, choose a number of months.

If the system determines that purging is necessary, it will purge both databases of data that is older than the number of months specified in this field.

Step 5   Click **Update**.

The new purge schedule configuration is added to the CRA system.

Configuring Purge Notification Parameters

When data is purged, the CRA system sends one of the following messages, depending on the activity that occurs:

- Database purged—Announces a purge has taken place, and includes an explanation of the purging activity.

- Database approaching maximum size—Sends an alert that the database is approaching its maximum size.

The system can send notifications through the following three methods:

- E-mail
- Syslog (system log)
- SNMP traps

For e-mail notification, the eMail subsystem must be configured on the CRA server. For information about configuring the eMail subsystem, see the "Provision the eMail Subsystem" section on page 6-13.

For Syslog and SNMP trap notification, the Cisco AVVID (Architecture for Voice, Video, and Integrated Data) Alarm Service must be running, and Syslog and SNMP must be properly configured. For more information about Cisco AVVID Alarm Service, Syslog, and SNMP, see the *Cisco Customer Response Applications Serviceability Guide*.

To configure the parameters of e-mail purge notification messages, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens.

Step 2   To change the purge notification parameters, click the **Purge Notification** hyperlink on the Historical Reporting Configuration navigation bar**.**

The Purge Notification area opens.

Step 3   In the Send Email Notifications To field, enter the e-mail address to which you want the notification sent.

Step 4   From the Send Email Notification When Database Size Exceeds *N* % of *maximum DB size* drop-down menu, accept the default of **85**, or choose another number.

Step 5   From the Initiate an Automatic Purge When Database Size Exceeds *N* % of *maximum DB size* drop-down menu, accept the default of **95**, or choose another number.

Step 6   From the Auto Purge Data for the Oldest *N* Days drop-down menu, accept the default of **7**, or choose another number.

Step 7   Click **Update.**

The Purge Notification area refreshes, and the CRA system is configured with the new values.

Purging Manually

You can manually purge the databases at any time. This action will not affect the automatic purging schedule.

A log file, Jvm.stdout, stores information about the manual purge activities that you perform. The Jvm.stdout file has no maximum size; when new information is generated, the information is appended to the existing jvm.stdout file. This log file is stored on the CRA server in the *<CRAinstallationDirectory>*\wfavvid\log\Purge_Sch directory. (By default, the system installs in the Program Files directory. You can view this log file by opening the file in a text editor.

To manually purge historical data, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **Tools > Historical Reporting**.

The Historical Reporting Configuration web page opens.

Step 2   Click the **Purge Now** hyperlink on the Historical Reporting Configuration navigation bar.

The Purge Now area opens.

Step 3   From the Purge Data Older Than *N* Months drop-down menu, accept the default number of **13**, or choose a different number.

The system will purge both databases of data that is older than the number of months that you specify.

Step 4   Click **Purge Now**.

The databases are purged, and the Purge Now area refreshes.

Truncating Database Transaction Log Files

The db_cra_log.ldf and dba_cra_ccdr_log.ldf database transaction log files can grow large. These log files are stored in the *<CRAinstallationDirectory>*\wfavvid directory on the CRA server, and also on the Historical Reports Database server if it is installed.

This Cisco CRA command line tool named **runTruncateHistDBLogs** can truncate either or both of these files to the size that you specify. You can run this command from a Microsoft Windows command window.

The process of truncating transaction log files can take up to 10 minutes.

Note   The runTruncateHistDBLogs command can spend up to 5 minutes per database log file performing the truncation. If you are substantially truncating a log file, this time limit may not allow the command to truncate the log file to the size that you specified. In this case, rerun the runTruncateHistDBLogs command to truncate the log files to the desired size.

To ensure that the truncated log files are updated with current information, perform a complete backup of the CRA databases and log files after executing the runTruncateHistDBLogs command.

The syntax for the runTruncateHistDBLogs command is:

runTruncateHistDBLogs *"dbUserName" "dbPassword"* {**"db_cra"** | **"db_cra_ccdr | "db_cra_all" | "tempdb"**} *size*

Table 9-3 lists the options and parameters for the runTruncateHistDBLogs command.

Table 9-3   Options and Parameters for runTruncateHistDBLogs

Option or Parameter	Description
"dbUserName"	User name of the database.
"dbPassword"	User password for the user name.
"db_cra"	Truncates the db_cra_log.ldf database transaction log file.
"db_cra_ccdr"	Truncates the db_cra_ccdr_log.ldf database transaction log file.

Table 9-3   Options and Parameters for runTruncateHistDBLogs (continued)

Option or Parameter	Description
"db_cra_all"	Truncates the db_cra_log.ldf and the db_cra_ccdr_log.ldf database transaction log files.
"tempdb"	Truncates the tempdb.ldf database transaction log file.
size	Size in MB to which the file or files will be truncated.
	It is recommended that, for the ldb_cra_log.ldf file, you specify a size no less than one-fourth the size of the ldb_cra.mdf database. It is recommended that, for the db_cra_ccdr_log.ldf log file, you specify a size no less than one-fourth the size of the db_cra_ccdr.mdf database.

Examples:

The following command truncates the db_cra_log.ldf database transaction log file to 250 MB:

runTruncateHistDBLogs "sa" "sa_password" "db_cra" 250

The following command truncates the db_cra_log.ldf and the db_cra_ccdr_log.ldf database transaction log files to 300 MB:

runTruncateHistDBLogs "sa" "sa_password" "db_cra_all" 300

Importing Historical Data from Data Files

If the local historical database on the CRA server is down, historical records are cached to be written to the database. If the number of records exceeds the cache maximum, the additional records are written to files stored in the **wfaavid\SQLdata** directory. These data files are also generated if the historical record queue is exceeded when the local historical databases on the Historical Reports Database server and CRA server are down.

You can import the data from these files into the historical database by running the **osql** command for all data files in the wfavvid\SQLData directory.

The syntax for the **osql** command is:

osql -U*userId* **-P***password* **-i***data_file_name*

Table 9-4 lists the options and parameters for the osql command on the CRA server.

Table 9-4   Options and Parameters for osql command

Option or Parameter	Description
userId	User id for the database.
password	User password for the user id.
data_file_name	Name of the file to be imported to database.

Example:

If the userId and password are "sample" and the file name is sampleFile.data, the command is:

osql -Usample -Psample -isampleFile.data

Importing Historical Data from Data Files

Managing the Cisco CRA Engine

Managing the Cisco CRA engine involves the following tasks:

- Viewing the engine status
- Starting and stopping the engine
- Configuring tracing
- Viewing tracing log files

You must be logged into CRA Administration to perform these tasks.

Note You should not modify the Cisco CRA Engine configuration unless instructed to do so by a Cisco technician.

This section describes:

Viewing the CRA Engine Status

You can view the status of the engine and CRA subsystems. You also can enable automatic refreshes of the engine status information and specify the refresh interval, in seconds. Automatic refresh enables you to view changes in the engine and subsystem status, which is especially useful when stopping or starting the engine.

For descriptions of each engine and subsystem state, see The Engine Status Hyperlink, page 14-10.

To view CRA Engine status, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **System > Engine**.

The Engine Configuration Web page opens, displaying the Engine Status area.

Step 2   View the status of the CRA Engine and subsystems.

Step 3   Enable automatic refresh of the status information by checking the Auto-refresh every *N* seconds check box. If you need to change the interval time, type the number into the Auto-refresh every *N* seconds text field.

The Engine Status page refreshes at the selected intervals.

Starting and Stopping the CRA Engine

You may need to stop and restart the CRA Engine. For example, you must stop the CRA Engine before modifying the Historical Reporting configuration, and restart the Engine for the changes to take effect. You may also stop and restart the CRA Engine to view the status of the Engine and subsystems while the Engine stops and starts.

Note   You can also control the CRA Engine from the Windows Service window, which you can open by choosing **Start > Programs > Administrative Tools > Services** from the Windows Start menu.

To stop or restart the CRA Engine, complete the following steps.

Procedure

Step 1   From the CRA Administration menu bar, choose **System > Engine**.

The Engine Configuration Web page opens, displaying the Engine Status area.

Step 2   Click **Start** to start the CRA Engine, or **Stop** to stop the CRA Engine.

Changing the IP Address of the CRA Server

To change the IP address for the server on which the CRA Engine resides, complete the following steps.

Procedure

Step 1   From the Cisco CRA Administration menu bar, choose **System > Engine**, click Stop Engine in the Engine web page, and then exit Cisco CRA Administration.

Step 2   Change the IP address on the Cisco CRA server to the new address.

Step 3   Reinstall and configure Cisco CRA 3.1. (Do not uninstall Cisco CRA 3.1 before reinstalling it.) Make sure to also install the latest Service release. Do not reinstall the Speech Server now.

Note   Refer to *Getting Started with Cisco Customer Response Applications* for installation instructions. Also see the "Installing a Required Service Release" section in the *Release Notes*.

Step 4   From the Cisco CRA Administration menu bar, choose **System > Engine**, click the **Engine Configuration** hyperlink, enter the new Cisco CRA server IP address in the Application Engine Hostname field, and then click **Update**.

Step 5   If you are using Cisco ICD, follow the procedure described in the "Updating the CAD Servers' IP Address" section in *Cisco Desktop Product Suite 4.5 (ICD) Service Information*.

Step 6   If you are using the Cisco IP Phone Agent service on Cisco CallManager, update the information in the Service URL field in the Cisco CallManager Administration Cisco IP Phone Services Configuration page with the new Cisco CRA server IP address.

Step 7   If you are using Cisco CRA Historical Reports:

    a. Stop the Cisco CRA Engine (see Step 1).

    b. From the Cisco CRA Administration menu bar, choose **Tools > Historical Reporting**, click the **Database Server Configuration** hyperlink, and then click **Update**.

    c. Start the Historical Reports Client, click **Server** in the Login dialog box, and change the server IP address to the new Cisco CRA server IP address.

Step 8   If you are using the ICM subsystem on the Cisco CRA Server, change the VRU PIM configuration to point to the new Cisco CRA Server IP Address.

Step 9   On each client computer from which you run real-time reports, point the web browser to the new Cisco CRA Server IP Address.

Step 10   If you have installed Nuance ASR on one or more dedicated servers, follow these steps on each such dedicated server:

    a. Choose **Start > Programs > Administrative Tools > Data Sources (ODBC)**.

    b. Click the **System DSN** tab.

    c. Click **wfnuance** in the System Data Sources pane and click **Configure**.

    d. In the Server field, type in the new IP address of the Cisco CRA Server and then click **Next**.

    e. In the Microsoft SQL Server DSN Configuration dialog box, make sure that this radio button is selected: With SQL Server authentication using a login ID and password entered by the user.

    f. Also in the Microsoft SQL Server DSN Configuration dialog box, enter nuance in the password field and then click **Next**.

    g. Click **Next** on the next dialog box that appears.

    h. Click **Finish** on the next dialog box that appears.

    i. In the ODBC Microsoft SQL Server Setup dialog box, click **Test Data Source** and verify that the operation completes successfully.

    j. Click **OK**.

> ✎
>
> **Note**   You do not need to take any action for Nuance TTS.

Step 11   Reboot the Cisco CRA Server.

> ✎
>
> **Note**   Before logging in to the Cisco Agent Desktop or in to the Cisco
> Supervisor Desktop, choose Start > Run on the computer on which you
> are running either of these programs and enter the following command,
> where new_ip is the new IP address of the Cisco CRA server:
> \\new_ip\DESKTOP_CFG\desktop\.

Configuring a Network Share for TTS

The following message might appear when you attempt to configure a network
share for TTS:

```
Network share connection failed. [Bad username/pwd or Server
unreachable].
```

Follow these steps to successfully configure the network share:

Step 1   Select **Start > Programs > Administrative Tools > Services**. The Services
window appears.

Step 2   Configure the CiscoCRAServletEngine service:

    a.   Right-click on CiscoCRAServletEngine service and choose Properties.

    b.   Click the Log On tab and make sure that the **This account radio button** is
checked and that the account is set to Administrator.

    c.   Click **OK**.

Step 3   Configure the Cisco CRA Engine service:

    a.   Right-click on Cisco CRA Engine service and choose Properties.

    b.   Click the Log On tab and make sure that the **This account radio button** is
checked and that the account is set to Administrator.

   c. Click OK.

Configuring Tracing

You can configure the CRA Engine trace files and trace level options. Tracing enables you to monitor CRA Engine and subsystem activity.

Note If you activate tracing, monitor the CPU usage and available disk space on the server. CPU usage near 100% or a full disk can cause your system to shut down unexpectedly.

Access tracing configuration by choosing **System > Engine** from the CRA Administration menu and clicking the **Trace Configuration** hyperlink.

For instructions on configuring tracing, refer to the *Cisco Customer Response Applications Serviceability Guide*.

Viewing Tracing Log Files

You can access tracing log files, which enable you to view CRA Engine and subsystem activity, through the CRA Administration.

To view tracing log files, complete the following steps.

Procedure

Step 1 From the CRA Administration menu bar, choose **System > Engine**.

The Engine Configuration Web page opens, displaying the Engine Status area.

Step 2 On the Engine navigation bar, click the **Trace Files** hyperlink.

The Trace Files area opens.

Step 3 Click the name or an attribute of the log file that you want to view.

The log file opens in a separate window.

For more information about the tracing log files, refer to the
Cisco Customer Response Applications Serviceability Guide.

■   **Viewing Tracing Log Files**

Reporting on Real-time CRA Data

When the CRA system is configured and functioning, you can run reports to monitor real-time activity using the CRA Administration web interface.

If you have the Cisco Agent Desktop and Cisco Supervisor Desktop, you also can run real-time reports directly from these applications. Cisco Agent Desktop and Cisco Supervisor Desktop do not use the same calculations or data display methods as those that CRA real-time reporting uses. Therefore, a report run using CRA real-time reporting and a report run using Cisco Supervisor Desktop may not display the same information for a given statistic. To avoid confusion, it might help to make one of these tools your standard reporting tool.

You must be logged into the CRA Administration web interface to run CRA real-time reports.

This section describes:

Available CRA Real-time Reports

CRA real-time reporting provides up to 11 reports that you can use to monitor CRA system activity. Table 11-1 briefly describes each of these reports. For detailed information about the data presented in each report, see The Report Menu, page 18-7.

Table 11-1   Available Real-time Reports

Report	Description
Application Tasks	Provides information about currently active applications.
Application Tasks Summary	Provides a summary of specific applications' activity.
Applications	Provides a list of all applications loaded on the CRA server.
Contact Summary	Provides information for call contacts, e-mail contacts, and HTTP contacts. Also provides the total number of contacts.
Contacts	Provides information about currently active contacts.
CSQ IP ICD Stats	Provides information about CSQ activity. This report is available only if IP ICD has been configured.
Datasource Usage	Provides information about configured datasource names (DSNs).
Engine Tasks	Provides information about currently active Engine tasks.
Overall IP ICD Stats	Provides information about ICD resources and calls. This report is available only if IP ICD has been configured.
Resource IP ICD Stats	Provides information about ICD resources activity.
Sessions	Provides information on all active sessions.

Opening Real-time Reporting

Real-time reporting is available from the CRA Administration web interface.

To open real-time reporting, complete the following steps.

Procedure

Step 1   Log into CRA Administration, if you are not already logged in.

Step 2   Choose **Tools > Real-time Reporting** from the CRA Administration menu.

The Application Reporting web page opens in a new window. The real-time reporting tool requires a Java plug-in. If the plug-ins is not installed on the machine you are using, the CRA system prompts you to accept the automatic installation of the plug-in. If you do not accept the installation, you cannot use Real-Time reporting.

You run real-time reports from the Application Reporting web page.

Running Reports

Open the real-time reporting tool from the CRA Administration web interface to run reports.

To run a real-time report, complete the following steps.

Procedure

Step 1   From the Application Reporting menu bar, choose **Reports**.

Step 2   From the Reports menu, choose the report to run.

The report opens in the Application Reporting window.

Viewing Detailed Subreports

You can view more detailed information for selected items in these four reports:

- Application Tasks report
- Contacts report
- Applications report
- Sessions report

To view detailed subreports, complete the following steps.

Procedure

Step 1   Run the Application Task, Contacts, Applications, or Sessions report.

Step 2   Click a line in the report for which you want to view more detailed information. For example, click an e-mail address in the Contacts report.

Step 3   From the Application Reporting menu bar, choose **Views** and click the subreport that you want to run.

You can also open a subreport by right-clicking on the selected item and choosing a subreport.

The subreport opens.

Resetting Report Statistics

The CRA system automatically resets all statistics each day at midnight. You can reset the accumulated statistics manually at any time. Resetting statistics does not reset active statistics, such as active contacts and active tasks.

To reset report statistics, complete the following steps.

Procedure

Step 1   From the Application Reporting menu bar, choose **Tools > Reset All Stats**.

The Reset Stats dialog box opens for you to confirm the reset.

Step 2   Click **Yes**.

Accumulated statistics are reset.

Printing Reports

To facilitate printing, you can open a printable version of a report.

To print a report, complete the following steps.

Procedure

Step 1   Run a report.

Step 2   From the Application Reporting menu, select **Tools > Open Printable Report**.

A printable version of the report opens in a separate window.

Step 3   Print the report using your browser's print functionality.

Setting Report Options

You can set the following reporting options:

- Refresh interval

- Number of times that the CRA Administration web interface should attend to reconnect to the CRA server.

- Whether logged off users appear in reports

To set report options, complete the following steps.

Procedure

Step 1   From the Application Reporting menu bar, choose **Settings > Options**.

Step 2   The Options dialog box opens.

Step 3   From the Polling Interval drop-down menu, choose the refresh rate in seconds.

Step 4   From the Server Connect Retry Count drop-down menu, choose the number of times that the CRA Administration web interface should attempt to reconnect to the CRA server.

Step 5   From the Show Logged Off Resources drop-down menu, choose whether logged off agents appear in reports.

Step 6   Click **Apply** to apply the settings.

Setting Report Appearance

You can select from three report appearances:

- Windows, which displays reports in colors based on your Windows settings
- Motif, which displays reports in purple and menu items in brown
- Metal, which displays reports in grey and menu items in black

To set the report appearance, choose **Settings** from the Application Reporting menu bar and click the appearance that you want.

Updating the JTAPI Client

The Cisco CRA server, Cisco Agent Desktop, and Cisco CallManager communicate using the JTAPI Client. CRA installation automatically detects the JTAPI Client used by the specified Cisco Call Manager server and installs this JTAPI Client on the CRA server.

If you change versions of Cisco CallManager after installing CRA, Cisco CallManager may use a different version of the JTAPI Client than the version used by the CRA server. The JTAPI Client Update Tool enables you to update the JTAPI Client on the CRA server and Cisco Agent Desktop to the same JTAPI Client version used by Cisco CallManager

The JTAPI Client Update Tool is installed by default in the C:\Program Files\wfavvid directory and is accessible from the Windows Start menu under Programs > Cisco CRA Administration.

You do not need to be logged into CRA Administration to update the JTAPI Client.

To update the JTAPI Client, complete the following steps.

Procedure

Step 1   From the Windows Start menu, choose **Programs > Cisco CRA Administration**.

Step 2   Choose **JTAPI Update Tool**.

The JTAPI Update wizard opens.

Step 3   Click **Next**.

Step 4   Enter the host name or IP address of the Cisco CallManager, the Windows user name for the administrator account on the Cisco CallManager server, and the administrator's Windows password for the Cisco CallManager server.

Step 5   Click **Next**.

The JTAPI Client Update Wizard opens.

Step 6   Click **Next** to proceed through the wizard.

A window opens, which lists the versions of JTAPI Client software used by the CRA server and Cisco CallManager. If the versions are the same, click **Exit**.

Step 7   If the versions are different, ensure that the Update JTAPI for Agent Desktops option is checked and click **Next**.

The JTAPI Client is installed. (If the JTAPI Client version on the CRA server is a later release than the version on Cisco CallManager, the JTAPI Client Update Tool first uninstalls the existing JTAPI Client from the CRA server and then installs the new JTAPI Client.)

The Finished Updating JTAPI window opens.

Step 8   Click **Exit**.

Step 9   Restart the CRA Engine for the update to take effect by either:

- Choosing **System > Engine** from the CRA Administration menu bar.

  The Engine status page opens.

  Click **Stop Engine**. When the CRA Engine has stopped, click **Start Engine**.

- Restarting the CRA Engine from the Windows Service window, which you can open by choosing **Start > Programs> Administrative Tools >Services** from the Windows Start menu.

Agents must restart their Cisco Agent Desktops for the JTAPI Client update to take effect.

CISCO SYSTEMS

P A R T   3

Cisco Customer Response Applications: Reference

Overview of the CRA Administration Web Interface

The Cisco Customer Response Applications (CRA) system provides a multimedia (voice, data, and web) IP-enabled customer-care application environment, using Voice over IP (VoIP) technology that allows your telephony network to share resources with your data network.

You can load your CRA system on an application server anywhere on the IP network. You can then use a web browser located on any computer on the IP network to configure and administer your applications with the CRA Administration web interface.

The CRA Administration web interface allows you to configure and monitor overall system functions, applications, and subsystems; access a wide variety of system tools; and perform many other administrative tasks.

This chapter provides an overview of the CRA Administration web interface, and includes the following sections:

The CRA Administration Web Interface

The web pages of the CRA Administration web interface allow you to configure and manage the CRA system and its subsystems.

> **Note**   For information about connecting to the Cisco CRA Administration web interface, see Connecting to the Cisco CRA Administration Web Interface for the First Time, page 3-2.

The CRA Administration Menu Bar and Menus

The CRA Administration menu bar, which appears at the top of every web page of the CRA Administration web interface, contains six menu options. You begin every CRA configuration and administration task by choosing a menu and submenu option from the menu bar.

The CRA Administration menu bar contains the following six menu options:

- **System**—Contains options for changing configuration and repository information, viewing the status of the CRA Engine and controlling CRA Engine activities, changing system parameters, and logging out of the CRA Administration web interface. For a description of all System menu options, see Chapter 14, "The System Menu."

- **Applications**—Contains options for configuring and refreshing applications. For a description of all Applications menu options, see Chapter 15, "The Applications Menu."

- **Scripts**—Contains options for managing and refreshing CRA scripts that are stored in the repository. For a description of all Scripts menu options, see Chapter 16, "The Scripts Menu."

- **Subsystems**—Contains options for configuring parameters for the subsystems that are licensed for your CRA server. Your menu may include submenu options for one or more of the following subsystems: Java Telephony Application Programming Interface (JTAPI), Integrated Contact Distribution (ICD), Intelligent Contact Management (ICM) software, Database, HTTP, eMail, Cisco Media, Nuance Automatic

Speech Recognition (ASR), and Nuance Text-To-Speech (TTS). For a description of all Subsystem menu options, see Chapter 17, "The Subsystems Menu."

- **Tools**—Contains options that allow you to access the following system tools: Alarm Definition, Plug-ins, Real-time Reporting, Real-time Snapshot Config, Historical Reporting, Prompt Management, Spoken Name Upload, User Maintenance, and Troubleshooting Tips. For a description of all Tools menu options, see Chapter 18, "The Tools Menu."

- **Help**—Provides access to online help for Cisco CRA. For a description of all Help menu options, see Chapter 19, "The Help Menu."

CRA Configuration Web Pages

When you choose any menu and submenu option from the CRA Administration menu bar, a configuration or administration web page opens. You use this web page to continue your configuration or administration task.

In some cases you will perform your configuration or administration task on this one web page. For example, you configure HTTP trigger information on the HTTP Trigger Configuration web page. (See Figure 13-1.)

Figure 13-1   HTTP Trigger Configuration Web Page

In other cases, the web page that first opens when you choose a submenu item leads to a series of web pages and areas of web pages. For example, Figure 13-2 shows the JTAPI Call Control Group Configuration web page, which contains both a navigation bar with hyperlinks that link to other web pages and a configuration area with hyperlinks that link to other web pages.

Figure 13-2   JTAPI Call Control Group Configuration Web Page

In some cases, each web page has a unique name. In other cases, configuration web pages retain the same title, but new areas appear when you click a hyperlink.

Using the Navigation Bar

On the left side of many web pages, you will find a navigation bar, which contains hyperlinks to other web pages. For example, as shown in Figure 13-2, the navigation bar of the JTAPI Call Control Group Configuration web page contains hyperlinks for the JTAPI Provider, CTI Port Groups, and JTAPI Triggers configuration web pages.

Using the "Add a New . . ." Hyperlink

In addition to displaying current configuration information, many web pages contain an **Add a New . . .** hyperlink that provides access to a web page that you can use to add new information.

For example, the JTAPI Call Control Group Configuration web page (shown in Figure 13-2) contains an **Add a New JTAPI Call Control Group** hyperlink. When you click this hyperlink, another area of the JTAPI Call Control Group Configuration web page opens. You can use this area to add a new JTAPI Call Control Group.

Using Other Hyperlinks and Buttons

In addition to the **Add a New . . .** hyperlink, many web pages contain other hyperlinks. For example, as shown in Figure 13-2, you can click the information under the column headings of the JTAPI Call Control Group Configuration web page to access and modify the configuration web page for that information.

Many web pages also contain buttons that perform a variety of functions. Figure 13-2, for example, shows the **Reload All** button on the JTAPI Call Control Group Configuration web page, which you can click to reload all the JTAPI call control group configurations in the CRA server.

The System Menu

The System menu of the Cisco Customer Response Applications (CRA) Administration system provides options for performing system-related tasks such as managing configuration and repository information, viewing and controlling CRA Engine activities, changing system parameters, and logging out of the CRA Administration web interface.

The System menu contains the following menu options:

- **Configuration and Repository**—Choose this option to change configuration and repository information.
- **Engine**—Choose this option to view the status of the CRA Engine and control CRA Engine activities.
- **System Parameters**—Choose this option to change system parameters.
- **Logout**—Choose this option to log out of the CRA Administration web interface.

This chapter includes the following sections:

The Configuration and Repository Menu Option

The Cisco CRA system stores configuration information in a Lightweight Directory Access Protocol (LDAP) directory called the IP telephony directory. Storing scripts and configuration information in an LDAP directory allows you to share applications and Cisco scripts among any CRA servers in the network.

You can use the Cisco CallManager Data Connection (DC) directory (included with the CRA system) as your IP telephony directory, or you can use an existing directory in your system (such as Netscape Directory or Microsoft Active Directory). The server that stores your IP telephony directory may be located on the same server on which the CRA system is installed or on a different server.

You can configure multiple directory servers to be used, in order of priority, if a failover occurs. Each of these directory servers stores Cisco CRA configuration data and scripts. If a failover occurs, the CRA server will attempt to use the first alternative directory server that you have configured, then the second server, and so on.

Each IP telephony directory contains a subdirectory that stores applications and Cisco scripts. This subdirectory is called the *repository.*The CRA server can receive directory information from one Cisco IP telephony directory and application configuration and script logic from a repository on another server. In this scenario, the directory and repository would have different configurations.

For efficient management of resources, the Cisco IP telephony directory server stores each type of configuration as a profile. In the event of a system failure or reallocation of CRA servers, you can upload a directory profile from the Cisco IP telephony directory to a replacement CRA server.

The Cisco IP telephony directory uses two kinds of profiles:

- Configuration profile—Stores all the configuration for a specific CRA server, such as groups, triggers, and subsystems.

- Repository profile—Stores information common to multiple CRA servers, such as scripts and application configuration.

Choose **System > Configuration and Repository** from the CRA Administration menu bar to access profile information and perform other configuration tasks related to the directory and repository servers. The Directory Setup web page opens.

Use the areas of the Directory Setup web page to configure the CRA server with your IP telephony directory location and required login parameters.

The navigation bar on the Directory Setup web page contains the following hyperlinks:

- **Configuration**—Click this hyperlink to display the Configuration Setup areas, which you use to set up and modify directory server information. (When the Directory Setup web page first opens, it displays the Configuration Setup—Step 1 of 2 area.)

- **Delete Configuration**—Click this hyperlink to display the List of Available Profiles area, which you use to view and delete configuration profiles.

- **Repository**—Click this hyperlink to display the Repository Setup areas, which you use to set up and modify repository server information.

- **Repository Initialization**—Click this hyperlink to display the Repository Initialization area, which you use to reload all the pre-packaged scripts and sample scripts in the repository and to make sure that initial information in the repository exists.

- **Delete Repository**—Click this hyperlink to display the List of Available Profiles area, which you use to view and delete profiles you create for the repository.

This section contains the following topics:

The Configuration Hyperlink

Click the **Configuration** hyperlink on the navigation bar of the Directory Setup web page to return to the Configuration Setup—Step 1 of 2 area from any other area of the Directory Setup web page.

(The Configuration Setup—Step 1 of 2 area automatically opens in the Directory Setup web page when you first choose the **Configuration and Repository** menu option from the System menu.)

Use the two Configuration Setup areas of the Directory Setup web page to set up and change information about your directory server.

Click **Next** to display the Configuration Setup—Step 2 of 2 area.

Table 14-1 and Table 14-2 show the fields of the two Configuration Setup areas (and the default values that appear if you have chosen to use the default DC Directory).

Table 14-1   Configuration Setup Area Fields—Step 1 of 2

Field	Description	Default for DC Directory
Server Type	Type of LDAP directory— MS Active Directory, Netscape Directory Server 4.0, or DC Directory.	DC Directory
Directory Host Name	Host name or IP address of the Cisco IP telephony directory server where the profile resides or where it will reside with the CRA Engine profile. The information entered in this field should be consistent with the information entered in the CTI Manager Area on the CTI Manager Locations pane during CRA installation To specify multiple directory servers in the event of a failover, after you enter the primary host name or IP address, enter the host names or IP addresses of the alternative directory servers in the order that they should be used if a failover occurs. Separate each host name or IP address in the Directory Host Name field with a semicolon (;), a comma (,), or a space. The information entered in this field should be consistent with the information entered in the CTI Manager B area on the CTI Manager Locations pane during CRA installation. **Note** The string "localhost" is not supported. Enter the host name or a valid IP address.	—
Directory Port Number	Port number of the Cisco IP Telephony directory.	8404

Table 14-1   Configuration Setup Area Fields—Step 1 of 2 (continued)

Field	Description	Default for DC Directory
Directory User (DN)	Username (called the distinguished name) configured on the directory server for the user with permission to modify the Cisco IP telephony tree and object entries.	cn=Directory Manager, o=cisco.com
Directory Password	Password for the directory user.	ciscocisco
User Base	Branch of the Cisco IP telephony directory tree that contains user information.	ou=Users, o=cisco.com
Base Context	Branch of the Cisco IP telephony directory tree that contains the Cisco configuration information.	o=cisco.com
Profile Name	Profile name that identifies this CRA server configuration or repository.	—

Table 14-2   Configuration Setup Area Fields—Step 2 of 2

Field	Description	Default for DC Directory
Profile Name	Profile name that identifies this CRA server configuration or repository.	—

Related Topic

- Setting up the IP Telephony Directory, page 3-3

The Delete Configuration Hyperlink

Click the **Delete Configuration** hyperlink on the navigation bar of the Directory Setup web page to view the configuration profiles that are available on your CRA system. The List of Available Profiles area opens. (See Figure 14-1).

Use the List of Available Profiles area to delete configuration profiles from the system.

Figure 14-1   Directory Setup Web Page—List of Available Profiles Area
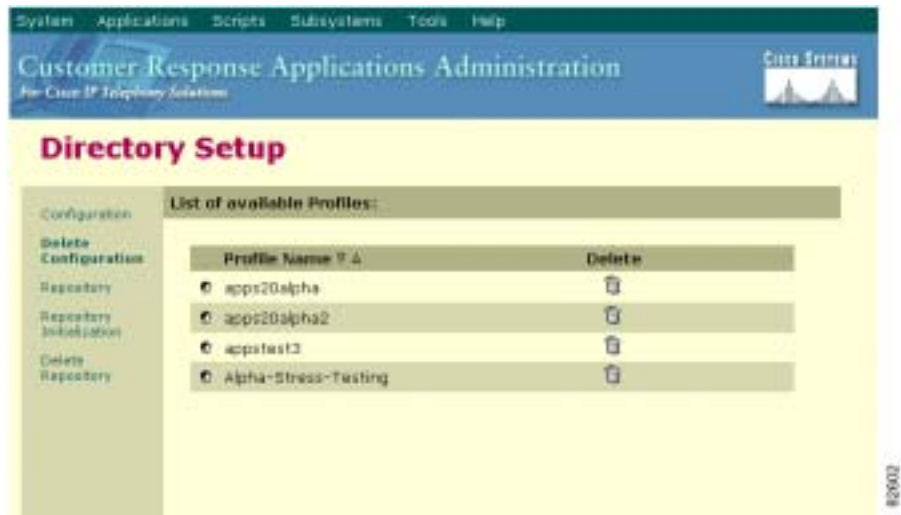
You can change the way that configuration profiles are listed in the List of Available Profiles area:

- To display the profiles in descending order, click the down arrow next to the Profile Name heading.
- To display the profiles in ascending order, click the up arrow next to the Profile Name heading.

To delete a configuration profile from the directory, click the **trash can** icon next to the name of the configuration profile that you want to delete.

> **Note**   To permanently remove a profile, you must delete it from both the directory and the repository. Use the **Delete Configuration** option to delete the profile from the directory and the **Delete Repository** option to delete the profile from the repository.

Related Topic

-

The Repository Hyperlink

Click the **Repository** hyperlink on the navigation bar of the Directory Setup web page to configure and modify repository server information. The Repository Setup—Step 1 of 2 area opens.

Use the two Repository areas to set up and change information about your repository server.

Click the **Next** button to display the Repository Setup—Step 2 of 2 area.

Table 14-3 and Table 14-4 show the fields of the two Repository Setup areas (and the default values that appear if you have chosen to use the default DC Directory).

Table 14-3   Repository Setup Area Fields—Step 1 of 2

Field	Description	Default for DC Directory
Server Type	Type of LDAP directory— MS Active Directory, Netscape Directory Server 4.0, or DC Directory.	DC Directory
Directory Host Name	Host name or IP address of the Cisco IP telephony directory server where the profile resides or where it will reside with the CRA Engine profile. **Note** The string "localhost" is not supported. Enter the host name or a valid IP address.	—
Directory Port Number	Port number of the Cisco P telephony directory.	8404

Table 14-3   Repository Setup Area Fields—Step 1 of 2 (continued)

Field	Description	Default for DC Directory
Directory User (DN)	Username (called the distinguished name) configured on the directory server for the user with permission to modify the Cisco IP telephony tree and object entries.	cn=Directory Manager, o=cisco.com
Directory Password	Password for the directory user.	ciscocisco
Base Context	Branch of the Cisco IP telephony directory tree that contains the Cisco configuration information.	o=cisco.com

Table 14-4   Repository Setup Area Fields—Step 2 of 2

Field	Description	Default for DC Directory
Profile Name	Profile name that identifies this CRA server configuration or repository. Click the **Edit** button to display a dialog box you can use to edit a profile or add a new profile to the Profile Name field.	—

Related Topic

The Repository Initialization Hyperlink

Click the **Repository Initialization** hyperlink on the navigation bar of the Directory Setup web page to re-initialize the repository. (You may need to re-initialize the repository if for some reason some of the prepackaged or sample scripts have been deleted, or if initial configuration information has been deleted.)

The system displays a prompt indicating that the procedure can take some time and asking if you want to continue. (The procedure should be quick). To continue, click **OK**.

The system displays a window asking you to wait while the results are retrieved. The CRA system reloads all the prepackaged scripts and sample scripts in the repository.

When the process completes, the system displays the following message:

```
Workflow setup done
```

Related Topic

- Setting up the IP Telephony Directory, page 3-3

The Delete Repository Hyperlink

Click the **Delete Repository** hyperlink on the navigation bar of the Directory Setup web page to view the repository profiles that are available on your CRA system. The List of Available Profiles area opens, as shown in Figure 14-1.

Use the List of Available Profiles area to delete repository profiles from the system.

You can change the way repository profiles are listed in the List of Available Profiles area:

- To display the profiles in descending order, click the down arrow next to the Profile Name heading.

- To display the profiles in ascending order, click the up arrow next to the Profile Name heading.

To delete a profile from the repository, click the **trash can** icon next to the name of the profile that you want to delete.

Note To permanently remove a profile, you must delete it from both the repository and the CRA server on which configuration profiles are stored. Use the **Delete Repository** option to delete the profile from the repository and the **Delete Configuration** option to delete the profile from the CRA server.

Related Topic

- Setting up the IP Telephony Directory, page 3-3

The Engine Menu Option

Choose **System > Engine** from the CRA Administration menu bar to access the Engine web page. (See Figure 14-2.)

Use the areas of the Engine web page to perform a variety of Engine management tasks.

The navigation bar on the Engine web page contains the following hyperlinks:

- **Engine Status**—Click this hyperlink to display the Engine Status area, which you use to view system status and start and stop the CRA Engine.

- **Engine Configuration**—Click this hyperlink to display the Engine Configuration area, which you use to modify CRA Engine parameters.

- **Trace Configuration**—Click this hyperlink to display the Trace Configuration area, which you use to configure the CRA Engine trace file and set trace level options.

- **Trace Files**—Click this hyperlink to display the Trace Files area, which you use to view information about trace files, display trace files, and manually write to the thread dump trace file.

  For more information about trace files, refer to the *Cisco Customer Response Applications Serviceability Guide*.

This section contains the following topics:

The Engine Status Hyperlink

Click the **Engine Status** hyperlink on the navigation bar of the Engine web page to return to the Engine Status area from any other area of the Engine web page. (See Figure 14-2.)

(The Engine Status area automatically opens in the Engine web page when you first choose the **Engine** menu option from the System menu.)

Use the Engine Status area to view the status of the CRA system and its subsystems (if the CRA Engine is running), start and stop the CRA Engine, and control how often the system refreshes information.

Figure 14-2   Engine Web Page—Engine Status Area

The Engine Status area displays information about the CRA system and its subsystems.

Note   Status information displayed in the Engine Status area does not update as the status of the system or a subsystem changes. To see updated status information, click the **Engine Status** hyperlink. To change the rate at which the Engine Status area automatically refreshes information, see the "Controlling the Engine Status Display Refresh Interval" section on page 14-14.

Information about the system appears in two columns with the following headings:

- System—Name of the system.

- Status—Status or state of the system.

Table 14-5 describes the possible system status messages that can appear under the System heading.

Table 14-5   CRA System Status Messages

System Status Display	Description
Stopped	The CRA Engine is not running.
Starting	The CRA Engine is initializing.
Stopping	The CRA Engine is in the process of stopping.
Running	The CRA Engine is running.
Pause Pending	The CRA Engine is in the process of pausing.
Paused	The CRA Engine is paused.
Continue Pending	The CRA Engine is in the process of receiving a notification to continue.

Information about subsystems appears in two columns with the following headings:

- Subsystems—Name of the subsystem. This column shows "Unavailable" if the CRA Engine is stopped.

- Status—Status or state of the subsystem.

Table 14-6 shows the possible subsystem status messages that can appear under the Subsystem heading.

Table 14-6   Subsystem Status Messages

Subsystems Status Display	Description
Initializing	The subsystem is in the process of initializing itself.
Shutting Down	The subsystem is in the process of shutting down. **Note** Completion of a subsystem shutdown varies from subsystem to subsystem. While the Shutting Down state may be too quick to register for some subsystems, other subsystems may be in the Shutting Down state for a prolonged period of time.
Shutdown	The subsystem has completed the process of shutting down.
In Service	The subsystem initialized successfully and is serving with full functionality.
Partial Service	The subsystem detected at least one error during initialization and is serving with reduced functionality.
Out of Service	The subsystem failed to initialize or is not ready to serve for some other reason.

This section contains the following topics:

Cisco Customer Response Applications Administrator Guide

Starting and Stopping the CRA Engine

You can use the Engine Status area of the Engine web page to start and stop the CRA Engine.

Click the **Start Engine** button to start the CRA Engine, or click the **Stop Engine** button to stop the CRA Engine.

Note You can also control the CRA Engine from the Windows Service window, which you display by choosing **Start > Programs > Administrative Tools > Services**.

Related Topic

Controlling the Engine Status Display Refresh Interval

When you start or stop the CRA Engine from the Engine status area of the Engine web page, the CRA system refreshes the information in the Engine Status area at regular intervals so you can monitor the status of the system or subsystems while the CRA Engine is starting or stopping. By default, the CRA system updates information in the Engine Status area every three seconds for five minutes.

Related Topic

The Engine Configuration Hyperlink

Click the **Engine Configuration** hyperlink on the navigation bar of the Engine web page to access the Engine Configuration area, which displays information you specified during user profile creation. (See Figure 14-3.)

Note Do not change the default values in the CRA Engine Configuration area unless instructed to do so by a Cisco technician.

Use the Engine Configuration area to modify CRA Engine parameters for a selected profile.

Figure 14-3   Engine Web Page—Engine Configuration Area

Table 14-7 shows the fields of the Engine Configuration area.

Table 14-7   Engine Configuration Area Fields

Field	Description
Application Engine Hostname	Host name or IP address of the server on which the CRA Engine resides. Changing the host name or IP address requires restarting the CRA Engine. Change this value only if the host name or IP address of the server changes **Note** For more information, see "Changing the IP Address of the CRA Server" in Chapter 10, "Managing the Cisco CRA Engine."
RMI[1] Port Number	The port number used by the CRA Engine to serve RMI requests.
Maximum Number of Executed Steps	The maximum number of steps an application can execute before the CRA Engine terminates the script or application. This limitation is intended to prevent a script from running indefinitely. **Note** Do not change the default value.
Additional Tasks	This field gives you control over the creation of additional threads that the CRA server internally initializes based on the number of licensed IVR[2] ports. By default, this field is set to 0 when a profile is first created.

1. RMI = remote method invocation

2. IVR = Interactive Voice Response

Related Topic

- Setting up the IP Telephony Directory, page 3-3

The Trace Configuration Hyperlink

Click the **Trace Configuration** hyperlink on the navigation bar of the Engine web page to access the Trace Configuration area. (See Figure 14-4.)

Use the Trace Configuration area to configure the CRA Engine trace file and set trace level options.

Figure 14-4   Engine Web Page—Trace Configuration Area

For a description of the fields and buttons in the Trace Configuration area and an explanation of how to use this area, refer to the *Cisco Customer Response Applications Serviceability Guide*. This guide also defines each of the trace level options.

The Trace Files Hyperlink

Click the **Trace Files** hyperlink on the navigation bar of the Engine web page to access the Trace Files area. (See Figure 14-5.)

Use the Trace Files area to view information about trace files, display trace files, and manually write to the thread dump trace file.

Figure 14-5   Engine Web Page—Trace Files Area
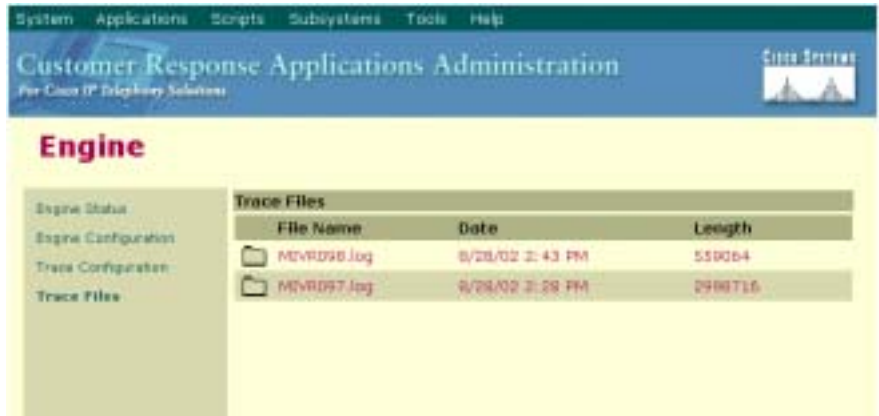
For an explanation of how to use the Trace Files area, refer to the *Cisco Customer Response Applications Serviceability Guide*.

The System Parameters Menu Option

Choose **System > System Parameters** from the CRA Administration menu bar to access the System Parameters Configuration web page.

Use the System Parameters web page to configure system parameters (including those that determine the locations from which prompts and grammars are loaded), configure the Real Time Transport Protocol (RTP) start port, and set the default session timeout.

Table 14-8 shows the fields of the System Parameters web page.

Table 14-8   System Parameters Web Page Fields

Field	Description
System Prompt Directory	Name of the directory that contains prompts that are used in internal Cisco modules and Cisco Packaged Applications. **Note** Do not modify this directory unless instructed to do so by Cisco technician.
User Prompt Directory	Name of the directory that contains the user prompts that are delivered with the system and the prompts that the user creates for the application.
Codec	The codec chosen during installation for this CRA server. The codec cannot be changed through CRA Administration.
System Grammar Directory	Name of the directory that contains the static grammars that are delivered with the system. **Note** Do not modify this directory unless instructed to do so by Cisco technician.
User Grammar Directory	Name of the directory that contains user-defined grammars stored in a user-specified directory.
RTP Start Port	RTP port number, which is used to send and receive media packets over the IP network. **Note** If your system is co-located with Cisco CallManager, this parameter must be set to 32256. Changing the default parameter value results in some calls being aborted by the system in an unspecified manner.
Default Language	System default language associated with new contacts for which no language has been defined. This field specifies the last possible fallback language when the system searches for resources such as prompts and grammars. The default entry for this field is "English (United States) [en_US]."

Table 14-8   System Parameters Web Page Fields (continued)

Field	Description
Default Currency	Default currency, such as American dollars (USD), French Francs (FRF), and so on.
	The system uses the default currency for converting currency amounts in a playable format when no currency designator is specified.
	The default entry for this field is "American Dollar [USD]."
Default TTS[1] Provider	Default TTS provider. If only one TTS provider is specified, it is selected as the default. If multiple TTS providers appear, the first installed TTS provider is set as the default.
Default Session Timeout	Maximum amount of time a user-defined session remains in memory after it becomes idle.
	The default entry for this field is "30" (minutes).

1. TTS = Text-to-Speech

Note   Changes you make on the System Parameters web page take effect immediately when you click **Update**, except for changes you make in the RTP Start Port field. If you change this field, you must stop and then start the CRA Engine. (See Starting and Stopping the CRA Engine, page 14-14.) All system parameters are stored on the CRA server (except for RTP Start Port) and are specific to the installation, so changing to a different profile will not alter these values.

Related Topic

- Install Grammars, page 7-16

The Logout Menu Option

You can exit CRA Administration by closing your web browser.

To exit CRA Administration without closing your web browser, choose **System > Logout** from the CRA Administration menu bar. The system logs you out of CRA Administration and displays the Authentication web page.

The Logout Menu Option

The Applications Menu

The Applications menu of the Cisco Customer Response Applications (CRA) Administration web interface contains options for configuring and refreshing applications.

The Cisco CRA system uses applications to interact with contacts and perform a wide variety of functions.

The Cisco CRA system uses the following types of applications:

- Cisco script applications—Based on scripts created in the CRA Editor, these applications perform functions such as receiving calls, playing back prompts, receiving caller input, transferring calls and queueing calls.

- Busy application—This application simulates a busy signal.

- Ring-No-Answer application—This application simulates a ring tone.

- ICM post-routing applications—With these applications, the Cisco IP Interactive Voice Response (IVR) system receives calls directly from Cisco CallManager, which sends calls to the post-routing route points on the Cisco CRA system.

- ICM translation-routing applications—With these applications, the CRA server is used as a queue point for Cisco IPCC (Contact Center), so that calls are routed by Cisco ICM to the CRA server.

The Applications menu contains the following menu options:

- **Configure Applications**—Choose this option to add, configure, copy, delete, or refresh a specific application.

- **Refresh Applications**—Choose this option to refresh all applications that are currently in use. (When you refresh an application, the system reloads the application from the repository to the CRA server.)

This chapter includes the following sections:

The Configure Applications Menu Option

You must configure applications in order to make them available to the CRA system.

Choose **Applications > Configure Applications** from the CRA Administration menu bar to configure applications. The Application Configuration web page opens.

Use the Application Configuration web page to add a new application and configure, copy, delete, or refresh an existing application,

The Application Configuration web page displays a list showing all the applications that are currently configured on the CRA server.

Table 15-1 shows the information and tools provided for each listed application.

Table 15-1   Application Configuration Web Page Column Headings

Column	Description	Notes
Name	Unique name of the application.	• Click the information in any of these columns to change configuration information for the application.
ID	Identifier of the application.	
Type	Type of application. (For a description of application types, see Chapter 7, "Configuring Cisco Script Applications," and Chapter 8, "Configuring Additional CRA Applications."	• Click the up or down arrow next to a column heading to sort applications in ascending or descending order by information in that column.
Sessions	Maximum number of simultaneous instances of the application that a single IVR system can run.	
Enabled	**Yes** if the application is enabled; **No** if the application is disabled.	
Copy	Allows you to make a copy of the application.	For more information, see the "Copy Icons" section on page 15-13.
Delete	Allows you to delete the application.	For more information, see the "Delete Icons" section on page 15-13.
Reload	Allows you to refresh the application.	For more information, see the "Reload Icons" section on page 15-14.

The main area of the Application Configuration web page contains the following hyperlinks:

- **Add a New Application**—Click this hyperlink to add a new application.

- **Application Name**—Click the name of a specific application to access the configuration page for this application.

- **Copy**—Click one of the **Copy** icons to copy a previously-existing application.

- **Delete**—Click one of the **trash can** icons to delete an application.

- **Reload**—Click one of the **Reload** icons to reload a previous version of an application.

This section contains the following topics:

- The Add a New Application Hyperlink, page 15-4

- Specific Application Name Hyperlinks, page 15-4

- Copy Icons, page 15-13

- Delete Icons, page 15-13

- Reload Icons, page 15-14

The Add a New Application Hyperlink

Click the **Add a New Application** hyperlink on the Application Configuration web page to upload (add) an application from the repository to the CRA server. The Add a New Application web page opens.

Use the Add a New Application web page to add an application to the CRA server.

To specify the type of the application to add, choose the application type from the drop-down menu of the Add a New Application web page, and then click **Next.**

A configuration web page opens that is specific to the application you choose.

Related Topics

- Add a Cisco Script Application, page 7-20

- Configure the Busy Application, page 8-3

- Configure the Ring-No-Answer Application, page 8-5

- Configure a Cisco ICM Post-Routing Application, page 8-8

- Configure a Cisco ICM Translation-Routing Application, page 8-11

Specific Application Name Hyperlinks

Click the hyperlinked name of a specific application displayed on the Application Configuration web page to configure that application. A type-specific configuration web page opens.

Use that configuration web page to enter such information as name, description, and the CRA script on which the application is based.

This section describes how to configure the following application types:

This section also describes how to add the following types of triggers:

Configuring Cisco Script Applications

Cisco script applications are based on scripts created in the CRA Editor. These applications perform functions such as receiving calls, playing back prompts, receiving caller input, transferring calls and queueing calls.

When you add a Cisco script application, or when you click the name of a specific Cisco script application displayed on the Application Configuration web page, the Cisco Script Application web page opens.

Use the Cisco Script Application web page to enter or modify configuration information.

Table 15-2 shows the fields of the Cisco Script Application web page.

Table 15-2   Cisco Script Application Web Page Fields

Field	Description
Name	Unique name of the application.
Description	Description of the application.
ID	Identifier of the application.
Maximum Number of Sessions	Maximum number of simultaneous calls or HTTP requests that the application can handle.
Enabled	Application is enabled/disabled.
Script	Script used by the application. **Note** When you select a script, the Cisco Script Application web page displays script-related parameters created with the CRA Editor. The administrator can modify these values. Each parameter has a check box, which enables you to override the default value. Check the check box to override the default value for that parameter.
Default Script	Script used to end the contact in the event that the primary script fails.

Related Topic

• Add a Cisco Script Application, page 7-20

Configuring Busy Applications

The Cisco Busy application simulates a busy signal to a caller when the desired extension is busy.

When you click the name of a specific Busy application displayed on the Application Configuration web page, the Busy Application web page opens.

Use the Busy web page to enter or modify configuration information.

Table 15-3 shows the fields on the Busy web page.

Table 15-3   Busy Web Page Fields

Field	Description
Name	Unique name of the application.
Description	Description of the application.
ID	Identifier of the application.
Maximum Number of Sessions	Maximum number of simultaneous calls or HTTP requests that the application can handle.
Enabled	Application is enabled/disabled.

Related Topic

• Configure the Busy Application, page 8-3

Configuring Ring-No-Answer Applications

The Ring-No-Answer application simulates a ring tone to a caller while the CRA system tries to connect the call.

When you click the name of a specific Ring-No-Answer application displayed on the Application Configuration web page, the Ring-No-Answer Application web page opens.

Use the Ring-No-Answer web page to enter or modify configuration information.

Table 15-4 shows the fields of the Ring-No-Answer web page.

Table 15-4   Ring-No-Answer Web Page Fields

Field	Description
Name	Unique name of the application.
Description	Description of the application.
ID	Identifier of the application.
Maximum Number of Sessions	Maximum number of simultaneous calls or HTTP requests that the application can handle.
Enabled	Application is enabled/disabled.

Related Topic

- Configure the Ring-No-Answer Application, page 8-5

Configuring Cisco ICM Post-routing Applications

With Cisco ICM post-routing applications, the Cisco IP IVR system receives calls directly from Cisco CallManager, which sends the calls to post-routing route points on the Cisco CRA system.

When you click the name of a specific Cisco ICM post-routing application displayed on the Application Configuration web page, the Cisco ICM Post-routing Application web page opens.

Use the Cisco ICM Post-routing Application web page to enter or modify configuration information.

Table 15-5 shows the fields on the Cisco ICM Post-routing Application web page.

Table 15-5   Cisco ICM Post-routing Application Web Page Fields

Field	Description
Name	Unique name of the application.
Description	Description of the application.
ID	Identifier of the application.

Table 15-5   Cisco ICM Post-routing Application Web Page Fields (continued)

Field	Description
Maximum Number of Sessions	Maximum number of simultaneous calls that the application can handle.
Enabled	Application is enabled/disabled.
Timeout	Number of seconds that the application waits for the next ICM instruction before timing out.
Initial Script	Script that the application runs when a call arrives.
Default Script	Script that the application runs in case of system problems.

Related Topic

- Configure a Cisco ICM Post-Routing Application, page 8-8

Configuring Cisco ICM Translation-routing Applications

With Cisco ICM translation-routing applications, the CRA server is used as a queue point for Cisco IPCC, so that calls are routed by Cisco ICM to the CRA server.

When you click the name of a specific Cisco ICM translation-routing application displayed on the Application Configuration web page, the Cisco ICM Translation-routing Application web page opens.

Use the Cisco ICM Translation-routing Application web page to enter or modify configuration information.

Table 15-6 shows the fields on the Cisco ICM Translation-routing Application web page.

Table 15-6   Cisco ICM Translation-routing Web Page Fields

Field	Description
Name	Unique name of the application.
Description	Description of the application.
ID	Identifier of the application.

Table 15-6   Cisco ICM Translation-routing Web Page Fields (continued)

Field	Description
Maximum Number of Sessions	Maximum number of simultaneous calls that the application can handle.
Enabled	Application is enabled/disabled.
Timeout	Number of seconds that the application waits for the next ICM instruction before timing out.
Default Script	Script that the application runs in case of system problems.

Related Topic

- Configure a Cisco ICM Translation-Routing Application, page 8-11

Adding a JTAPI Trigger

A Java Telephony Application Programming Interface (JTAPI) trigger responds to each call that arrives on a specific route point by selecting telephony and media resources to serve the call and then invoking an application script to handle the call.

You can add a JTAPI trigger to an application of any type.

To add a JTAPI trigger, click the name of any application displayed on the Application Configuration web page. The configuration web page specific to the application type opens.

Click the **Add New Trigger** hyperlink. The Add a New Trigger web page opens.

Choose JTAPI from the drop-down menu, and then click **Next**. The JTAPI Trigger Configuration web page opens.

Table 15-7 shows the fields of the JTAPI Trigger Configuration web page.

Table 15-7   JTAPI Trigger Configuration Web Page Fields

Field	Description
CTI Route Point Directory Number	Available CTI [use fn to expand acronym] route point (directory number) that is associated with the trigger.
Language	Default language to associate with the incoming call when the application is started.
Application Name	*Display only.* Name of the application associated with the trigger.
Maximum Number Of Sessions	Maximum number of simultaneous calls that the trigger can handle.
Idle Timeout	Maximum amount of time that the CRA system waits for all the required resources to process a call and to invoke the application before rejecting a call.
Enabled	Trigger is enabled/disabled.
Call Control Group	Call control group associated with the trigger.
Primary Dialog Group	Media dialog group associated with the trigger, if media is required by the associated application.
Secondary Dialog Group	Media dialog group used if the primary dialog group lacks enough resources to provide for an incoming call on this trigger.

Related Topics

- Add a JTAPI Trigger from the Cisco Script Application Web Page, page 7-22
- Add a JTAPI Trigger from the JTAPI Subsystem, page 7-23

Adding an HTTP Trigger

HTTP applications use triggers to activate applications in response to incoming HTTP messages. An HTTP trigger is the relative URL a user enters into the client browser to start the application.

To add an HTTP trigger, click the name of any application displayed on the Application Configuration web page. The configuration web page specific to the application type opens.

Click the **Add New Trigger** hyperlink. The Add a New Trigger web page opens.

Choose HTTP from the drop-down menu, and then click **Next**. The HTTP Trigger Configuration web page opens.

Table 15-8 shows the fields of the HTTP Trigger Configuration web page.

Table 15-8   HTTP Trigger Configuration Web Page Fields

Field	Description
URL	URL to associate the application with the HTTP trigger.
Language	Default language to associate with the incoming call when the application is started.
Application Name	*Display only.* Name of the application associated with the trigger.
Maximum Number Of sessions	Maximum number of simultaneous calls that the trigger can handle.
Idle Timeout (in ms)	Maximum wait time in milliseconds before the CRA system rejects the HTTP request for this trigger.
Enabled	Trigger is enabled/disabled.

Related Topic

- Adding an HTTP Trigger, page 7-25

Copy Icons

Click the **Copy** icon next to the name of any application displayed on the Application Configuration web page to copy that application. The configuration web page specific to the application type opens.

Use the application configuration web page to copy an application that already exists on the CRA server, in order to make a modification and save the modified copy as a new application under a new name.

From this configuration web page, you can modify configuration information, including the name of the application. When you click the Add button, the application configuration page refreshes, with the new application included.

Related Topic

Delete Icons

Click the **trash can** icon next to the name of any application displayed on the Application Configuration web page to delete that application. A dialog box asks you to confirm the deletion. When you click OK, the CRA system deletes the selected application.

Use the **Delete** icon to delete applications that are no longer used. When you delete an application, you permanently remove it from the repository and make it unavailable to the CRA system.

Related Topic

Reload Icons

Click the **Reload** icon next to the name of any application displayed on the Application Configuration web page to reload that application. The CRA system reloads the selected application from the repository to the CRA server.

Use the **Reload** icon to reload (or refresh) an application when, for example, you have modified any scripts or triggers that the application uses.

Note   The CRA Administration web interface uses the word "reload" as synonymous with the word "refresh" (which is more widely used.)

Related Topic

The Refresh Applications Menu Option

When you modify scripts, triggers, or other configuration information that applications use, you need to refresh these applications in order to instruct them to use the new information.

The Refresh Applications option lets you refresh all the applications that are currently being used, loaded, and managed by the Administration session and by the CRA server.

Choose **Applications > Refresh Applications** from the CRA Administration menu bar to refresh all applications. A CRA Administration web page opens, displaying the following message:

```
All applications have been successfully loaded.
```

C H A P T E R **16**

The Scripts Menu

The Scripts menu of the Cisco Customer Response Applications (CRA) Administration web interface contains options for managing and refreshing CRA scripts that are stored in the repository.

Cisco CRA applications are based on scripts created in the Cisco CRA Editor.

Your Cisco CRA system includes sample scripts stored as .aef files. These scripts have been built using Cisco CRA Editor steps, including prerecorded prompts. You can use these scripts to create applications without performing any script development, or you can use these scripts as models for your own customized scripts.

Note The included scripts are bundled with the CRA system solely as samples, and are not supported by Cisco. For more information on these sample scripts, refer to the *Cisco Customer Response Applications Developer Guide*.

Table 16-1 describes the sample CRA Editor scripts that may be included with your Cisco CRA system, depending on which product you have purchased.

Table 16-1   Sample Cisco CRA Scripts

Sample Script	Description
aa.aef	This basic Auto-Attendant script allows a caller to call a user by entering an extension number or the first few characters of an associated username. If ASR is enabled, the caller may simply speak the extension or the user name.
hotel.aef	This script allows a caller to log in remotely, and is used with Cisco Extended Services. See the *Cisco CallManager Extended Services Administrator Guide* for more information.
hotelout.aef	This script allows a caller to log out remotely, and is used with Cisco Extended Services. See the *Cisco CallManager Extended Services Administrator Guide* for more information.
icd.aef	This basic ICD[1] script establishes a simple call queue and routes callers to a group of agents as the agents become available. **Note** This file is included with Cisco IP ICD products only.
voicebrowser.aef	This Voice Browser script uses ASR functionality to allow a caller to access information from VoiceXML[2] -enabled web sites.
outboundVoiceBrowser.aef	This Voice Browser script allows the user to place outbound calls according to instructions stored in VoiceXML files.
SNU.aef	This script enables Cisco CallManager users to call in, authenticate their identities, and replace their spoken names with newly recorded announcements on their telephones.

1.   ICD = Integrated Contact Distribution

2.   VoiceXML = Voice eXtensible Markup Language

Table 16-2 describes the IP Queue Manager sample scripts that may be included with your CRA system.

Table 16-2   Sample Cisco CRA IP QM Scripts

Sample Script	Description
BasicQ.aef	This VRU[1] script greets a caller and puts the call on hold while waiting for an available agent.
VisibleQ.aef	This VRU script greets a caller, provides feedback about the estimated time until the caller will be connected, and puts the call on hold while waiting for an available agent.
CollectDigits.aef	This VRU script acquires an account number (or other numbers) from a caller.
CVInput.aef	This VRU script uses ICM[2] call variables to fully customize the Extended Get Digit String step to collect information from the caller and return it to the ICM script.
CVOutput.aef	This VRU script uses ICM call variables to fully customize the Extended Play Prompt step to play back information to the caller.
Input.aef	This VRU script is similar to the CVInput.aef script, except that it uses ICM expanded call variables to pass information for the customizing of the step.
Output.aef	This VRU script is similar to the CVOutput.aef script, except that it uses ICM expanded call variables to pass information for the customizing of the step.

1.   VRU = Voice Response Unit

2.   ICM = Intelligent Contact Management

The Scripts menu contains the following menu options:

- **Manage Scripts**—Choose this option to add a new script and to view, refresh, restore, upload, or delete an existing script.

- **Refresh Scripts**—Choose this option to refresh all scripts currently in use.

Cisco Customer Response Applications Administrator Guide

This chapter includes the following sections:

The Manage Scripts Menu Option

Choose **Scripts > Manage Scripts** from the CRA Administration menu bar to work with scripts. The Manage Scripts web page opens.

Use the Manage Scripts web page to add a new script and to view, refresh, restore, upload, or delete an existing script.

The Manage Scripts web page displays a list showing all scripts that have been uploaded to the repository. Table 16-3 shows the information and tools provided for each listed application.

Table 16-3   Manage Scripts Web Page Table Column Headings

Column	Description	Notes
Name	File name of the script. **Note** Click the up or down arrow next to this column heading to display applications in ascending or descending order by name.	Click the information in any of these columns to view or download the script file. For more information, see the "Specific Application Information Hyperlinks" section on page 16-6.
Last Modified	Date and time that the script was last uploaded to the repository. **Note** If the script has only been uploaded once, this field will display "Not available".	
Created	Date and time that the script was first uploaded to the repository.	
Refresh	Allows you to use the newest version of the script.	For more information, see the "Refresh Icons" section on page 16-7.

Table 16-3   Manage Scripts Web Page Table Column Headings (continued)

Column	Description	Notes
Restore in Repository	Allows you to replace a script in the repository with the previous version of the script.	For more information, see the "Restore Icons" section on page 16-7.
Upload to Repository	Allows you to upload a new version of an existing script to the repository.	For more information, see the "Upload Icons" section on page 16-7.
Delete	Allows you to delete a script from the repository.	For more information, see the "Delete Icons" section on page 16-8.

The main area of the Manage Scripts web page contains the following hyperlinks:

- **Add a Script**—Click this hyperlink to add a script to the repository.

- **Specific Application Information**—Click a hyperlinked script name or the information next to it to view or download that script.

- **Refresh**—Click the **Refresh** icon next to the name of a script to refresh that script.

- **Restore**—Click the **Restore** icon next to the name of a script to restore the previous version of that script.

- **Upload**—Click the **Upload** icon next to the name of a script to upload a new script.

- **Delete**—Click the **Delete** icon next to the name of a script to delete that script.

This section contains the following topics:

The Add a Script Hyperlink

Click the **Add a Script** hyperlink on the Manage Scripts web page to add a script to the repository. The Uploading Scripts window opens.

Use the Uploading Scripts window to upload a script to the repository.

Table 16-4 shows the fields in the Add New Script window.

Table 16-4   Add New Script Window Fields

Field	Description
Source Script Name	Name of the script that is the source for the script you want to add.
Destination Script Name	Name of the script as it will appear in the repository. Note You can use the same name as the source script name.

Related Topic

- Adding a Script, page 7-4

Specific Application Information Hyperlinks

Click the hyperlinked name of any script file that appears on the Manage Scripts web page, or the hyperlinked information next to it, to view or download that script. The File Download dialog box opens, from which you can view the script or choose a directory as a destination to download the script file.

Use the File Download dialog box to view or download any script that appears on the Manage Scripts page. This feature can be useful if you want to inspect a script or download a copy of a script in order to modify it.

Related Topic

- Viewing or Downloading a Script File, page 7-5

Refresh Icons

Click the **Refresh** icon next to the name of any script displayed on the Manage Scripts web page to refresh that script. The Refresh Script area opens.

Click **Yes** to refresh the script and all applications that reference the script, or click **No** to refresh the script only.

Use the Refresh Script area to instruct the CRA system to upload the newest version of a script to the CRA server when you modify that script.

Related Topic

- Refreshing a Script, page 7-6

Restore Icons

Click the **Restore** icon next to the name of any script displayed on the Manage Scripts web page to restore that script. A web page opens indicating that the script was restored successfully.

Use the **Restore** icon to replace the current version of a script with its previous version (similar to an Undo command). This feature can be useful if you make a change in a script, and then decide to use the previous version of the script instead.

Related Topic

- Restoring a Script, page 7-7

Upload Icons

Click the **Upload** icon next to the name of any script displayed on the Manage Scripts web page to upload a new script. The Upload Script area opens.

Use the Upload Script area to replace an existing script with a new script, but retain the name of the previous script.

Table 16-5 shows the fields in the Upload Script area.

Table 16-5   Upload Script Area

Field	Description
Source Script Name	Name of the script that is the source for the script you want to upload.
Destination Script Name	Name of the script as it appears in the repository.

Related Topic

Delete Icons

Click the **Delete** icon next to the name of any script displayed on the Manage Scripts web page to delete that script from the repository. A dialog box asks you to confirm the deletion. When you click OK, the CRA system deletes the selected script.

Use the **Delete** icon to delete scripts that are no longer used. When you delete a script, you permanently remove it from the repository and make it unavailable to the CRA system.

Related Topic

The Refresh Scripts Menu Option

When a script is modified, you must instruct the CRA system to load the newest version onto the CRA server by refreshing the script, so that all the applications and subsystems that use the script will use the newest version.

Choose **Scripts > Refresh Scripts** from the CRA Administration menu bar to refresh all scripts currently in use. The Engine web page opens, with a dialog box asking you whether or not you would like to reload all applications as well.

Use the Refresh Scripts menu option to refresh all the scripts currently in use.

Click **OK** to refresh all applications as well as all scripts, or click **Cancel** to refresh all scripts but no applications. The Engine web page displays a message showing that the operation was successful.

Related Topic

- Refreshing a Script, page 7-6

■ **The Refresh Scripts Menu Option**

The Subsystems Menu

The Subsystems menu of the Cisco Customer Response Applications (CRA) Administration web interface provides access to the subsystems that are licensed for your CRA system.

The CRA system uses subsystems for communicating with other services. Depending on the CRA package you have installed, the Subsystems menu may contain some or most of the following menu options:

- **JTAPI**—Choose this option to enter JTAPI provider information, CTI (Computer Telephony Interface) port group information, and JTAPI trigger information.

- **ICD**—Choose this option to set up your ICD (Integrated Contact Distribution) resources.

- **ICM**—Choose this option to configure the ICM (Intelligent Contact Management) subsystem to interact with Cisco ICM software and to add new VRU (Voice Response Units) scripts.

- **Database**—Choose this option to configure the CRA system to communicate with database servers.

- **HTTP**—Choose this option to configure the CRA Engine to respond to requests from a variety of web clients, including computers and IP phones.

- **eMail**—Choose this option to configure the CRA Engine to communicate with your e-mail server and enable your applications to create and send e-mail.

- **Cisco Media**—Choose this option to configure Cisco Media Termination (CMT) dialog groups that can be used to handle simple Dual-Tone Multi-Frequency (DTMF) based dialog interactions with customers.

- **Nuance ASR**—Choose this option to configure the Nuance Automated Speech Recognition (ASR) subsystem, which allows users to navigate through a menu of options using spoken responses to prompts.

- **Nuance TTS**—Choose this option to configure the Nuance Text-to-Speech (TTS) subsystem, which converts plain text (UNICODE) into spoken words in order to provide a user with information or to prompt a user to respond to an action.

This chapter includes the following sections:

The JTAPI Menu Option

The Cisco CRA system uses the Java Telephony Application Programming Interface (JTAPI) subsystem of the CRA Engine to send and receive call-related messages from the Cisco CallManager CTI (Computer Telephony Interface) Manager.

Choose **Subsystems > JTAPI** from the CRA Administration menu bar to configure the JTAPI subsystem. The JTAPI Configuration web page opens.

Use the areas of the JTAPI Configuration web page to enter JTAPI provider information, CTI port group information, and JTAPI trigger information.

The JTAPI Configuration navigation bar contains the following hyperlinks:

- **JTAPI Provider**—Choose this option to enter JTAPI provider information.
- **CTI Port Groups**—Choose this option to configure CTI port groups for applications.
- **JTAPI Triggers**—Choose this option to configure JTAPI triggers for applications.

This section contains the following topics:

The JTAPI Provider Hyperlink

Click the **JTAPI Provider** hyperlink on the navigation bar of the JTAPI Configuration web page to return to the JTAPI Provider area from any other area of the JTAPI Configuration web page.

(The JTAPI Provider area automatically opens in the JTAPI Configuration web page when you first choose the **JTAPI** menu option from the Subsystems menu.)

Use the JTAPI Provider area to enter the location of your JTAPI provider, user ID, and password.

Note   The JTAPI provider is the JTAPI user that you created in Cisco CallManager. (See Chapter 2, "Configuring Cisco CallManager for Cisco CRA.".)

Table 17-1 shows the fields of the JTAPI Provider area of the JTAPI Configuration web page.

Table 17-1   JTAPI Provider Area Configuration Fields

Field Heading	Description
JTAPI Provider	IP address or host name of the Cisco Media Convergence Server (Cisco MCS) running Cisco CallManager CTI Manager. **Note** You can enter up to two CTI Managers, separated by a space. If the first CTI Manager becomes unavailable, the second one connects and maintains calls.
User ID	Cisco CallManager UserID (for example, "JTAPI") that the CRA server will use to communicate with the JTAPI provider.
Password	Password you defined for the UserID in CallManager so that the CRA server can communicate with the JTAPI provider.

Related Topic

- Provision the JTAPI Subsystem, page 4-3

The CTI Port Groups Hyperlink

Click the **CTI Port Groups** hyperlink on the navigation bar of the JTAPI Configuration web page to access the first JTAPI Call Control Group Configuration area of the JTAPI Configuration web page.

Use the first JTAPI Call Control Group Configuration area to modify configuration information for existing JTAPI call control groups.

Table 17-2 shows the tabular information displayed in the first JTAPI Call Control Group Configuration area of the JTAPI Configuration web page.

Table 17-2   First JTAPI Call Control Group Configuration Area Columns

Column Heading	Description
Group ID	ID assigned to the group.
Description	Description of the group.
CTI Ports	Number of CTI Ports assigned to the group.
Copy	Allows you to make a copy of an existing group.
Delete	Allows you to delete a call control group.
Reload	Allows you to reload a call control group.

Table 17-3 describes the button in the first JTAPI Call Control Group Configuration area of the JTAPI Configuration web page.

Table 17-3   First JTAPI Call Control Group Configuration Area Button

Name	Description
Reload All	Reloads all the group configurations in the CRA server.

The first JTAPI Call Control Group Configuration area of the JTAPI Configuration web page also displays the number of licensed IVR ports, which is the total number of available Interactive Voice Response (IVR) ports licensed for this CRA system.

The main area of the first JTAPI Call Control Group Configuration area of the JTAPI Configuration web page contains the following hyperlinks:

- **Add a New JTAPI Call Control Group**—Click this hyperlink to add a new JTAPI call control group.

- **Specific Call Control Group Information**—Click a hyperlinked call control group name or the information next to it to access the configuration information for that call control group.

- **Copy**—Click the **Copy** icon next to the name of a call control group to copy the configuration information for this call control group.

- **Delete**—Click the **Delete** icon next to a specific call control group name to delete the call control group.
- **Reload**—Click the **Reload** icon next to the specific call control group name to reload the configuration information.

This section contains the following topics:

- Adding a New JTAPI Call Control Group, page 17-6
- Associating CTI Ports for this Group, page 17-8

Adding a New JTAPI Call Control Group

✎
Note Before you can add JTAPI call control groups, you must create a Cisco CallManager user for the JTAPI subsystem, create CTI ports and CTI route points, and associate the ports and route points with the JTAPI user. (See Chapter 2, "Configuring Cisco CallManager for Cisco CRA.")

When you click the **Add a New JTAPI Call Control Group** hyperlink in the first JTAPI Call Control Configuration area of the JTAPI Configuration web page, the second JTAPI Call Control Group Configuration area opens.

Use the second JTAPI Call Control Group Configuration area to add a new JTAPI call control group.

✎
Note If your system is co-located with Cisco CallManager, you can configure a maximum of 256 CTI ports in total for all CTI port groups. Configuring more CTI ports than this limit results in calls being aborted by the system in an unspecified manner.

Table 17-4 shows the fields in the second JTAPI Call Control Group Configuration area of the JTAPI Configuration web page.

*Table 17-4   Second JTAPI Call Control Group Configuration Area
Fields*

Field Heading	Description
Group ID	ID for the call control group in this field.
Description	Description for this group in this field.
Number of Licensed IVR Ports	*Display only.* Number of licensed IVR ports.
List of CTI Ports	CTI ports associated with the group.
Number of CTI Ports	Number of CTI ports associated with the group.
Calling Search Space for Redirect	Specifies the search space the calling device searches when attempting to redirect the call. Options are the following: • Call manager default—The redirect uses the search space that is the default for the implementation. • Calling party—The redirect uses the search space of the calling address. • Redirecting party—The redirect uses the search space of the redirect controller's address.

Table 17-5 describes the button in the second JTAPI Call Control Group
Configuration area of the JTAPI Configuration web page.

Table 17-5   Second JTAPI Call Control Group Configuration Area Button

Name	Description
Associate CTI Ports	Associates a CTI port group with a JTAPI call control group. (See Associating CTI Ports for this Group, page 17-8.)

Associating CTI Ports for this Group

When you click the **Associate CTI Ports** button on the second JTAPI Call Control Group Configuration area of the JTAPI Configuration web page, the Please Assign CTI Port for this Group area opens.

Use the Please Assign CTI Port for this Group area to associate a CTI port with a JTAPI call control group so that the call control group can use the CTI ports.

Note   The **Associate CTI Ports** button is enabled only if the CRA Engine is running.

Table 17-6 shows the fields in the Please Assign CTI Ports for this Group area of the JTAPI Configuration web page.

Table 17-6   Please Assign CTI Ports for this Group Columns

Column Heading	Description
Available CTI Ports List Filters	Filtering search mechanism that allows you to find available CTI ports.
Available CTI Ports	**Check All** button displays the CTI ports associated with the group; **Uncheck All** button displays the available CTI ports.
Directory Number and Device Name	Directory number and device name associated with the group.

Related Topic

- Provisioning JTAPI Call Control Groups, page 4-5

The JTAPI Triggers Hyperlink

Click the **JTAPI Triggers** hyperlink on the navigation bar of the JTAPI Configuration web page to configure JTAPI triggers to invoke application scripts in response to incoming contacts. The first JTAPI Trigger Configuration area opens.

Use the first JTAPI Trigger Configuration area to configure an existing application.

Table 17-7 shows the tabular information displayed in the first JTAPI Trigger Configuration area of the JTAPI Configuration web page.

Table 17-7   First JTAPI Trigger Configuration Area Columns

Column Heading	Description
Route Point	CTI Route Points (Directory Numbers).
Application	Name of the application.
Sessions	Maximum number of simultaneous instances of the associated application that can run when triggered by this trigger.
Enabled	True if the trigger is enabled; False if the trigger is disabled.
Copy	Allows you to make a copy of an existing trigger.
Delete	Allows you to delete a trigger.
Reload	Allows you to reload a trigger.

The main area of the first JTAPI Trigger Configuration area of the JTAPI Configuration web page contains the following hyperlinks:

- **Add a New JTAPI Trigger**—Click this hyperlink to access the second JTAPI Trigger Configuration area and add a new JTAPI trigger.

- **Specific Trigger Information**—Click a hyperlinked trigger or the information next to it to access its configuration information.

- **Copy**—Click the **Copy** icon to copy the trigger information.

- **Delete**—Click the **Delete** icon to delete the trigger.

- **Reload**—Click the **Reload** icon to reload the trigger configuration information.

This section contains the following topic:

- Adding a JTAPI Trigger, page 17-10

Adding a JTAPI Trigger

When you click the **Add a New JTAPI Trigger** hyperlink in the first JTAPI Trigger Configuration area of the JTAPI Configuration web page, the second JTAPI Trigger Configuration area opens.

Use the second JTAPI Trigger Configuration area to add a new JTAPI trigger.

Table 17-8 shows the tabular information displayed in the second JTAPI Trigger Configuration area of the JTAPI Configuration web page.

Table 17-8   Second JTAPI Trigger Configuration Area Columns

Fields or Drop-Down Arrow Heading	Description
CTI Route Point Directory Number	Available CTI route point, which is the directory number associated with the trigger.
Language	Default language to associate with the incoming call when the application is started.
Application Name	Application to associate with the trigger.
Maximum Number of sessions	Maximum number of simultaneous calls that the trigger can handle.
Enabled	True if the trigger is enabled; False if the trigger is disabled.
Call Control Group	Call control group to associate with the trigger.
Primary Dialog Group	Dialog group to associate with this trigger, if media is required by the associated application.
Secondary Dialog Group	Secondary dialog group to associate with this trigger, in case the primary dialog group does not have enough resources to provide for an incoming call on this trigger.

Related Topic

• Provisioning a JTAPI Trigger, page 4-7

The ICD Menu Option

The Cisco CRA system uses the ICD (Integrated Contact Distribution) subsystem of the CRA Engine to provide resource distribution and queueing to call centers, as part of a Automatic Call Distribution (ACD) system.

Choose **Subsystems > ICD** from the CRA Administration menu bar to set up your ICD resources. The ICD Configuration web page opens.

Use the areas of the ICD Configuration web page to configure skills groups, resources, resource groups, Contact Service Queues (CSQs) and RM (Resource Manager) JTAPI providers.

The ICD Configuration navigation bar contains the following hyperlinks:

- **Skills**—Click this hyperlink to create skills (This option is available only with the Cisco IP ICD Enhanced and Cisco IP ICD Enhanced with CTI Option products.)

- **Resources**—Click this hyperlink to assign a resource group and/or skills to agents.

- **Resource Groups**—Click this hyperlink to create resource groups.

- **Contact Services Queues**—Click this hyperlink to configure Contact Service Queues (CSQs).

- **RM JTAPI Provider**—Click this hyperlink to configure the RM (Resource Manager) JTAPI provider for the ICD subsystem.

- **Assign Skills**—Click this hyperlink to assign skills and/or a resource group to agents in bulk. (This option is available only with the Cisco IP ICD Enhanced and Cisco IP ICD Enhanced with CTI Option products.)

For details on the maximum number of agents, skills, and CSQs that you can configure on your system, see About IP ICD, page 5-2.

This section contains the following topics:

The Skills Hyperlink

Note   The **Skills** hyperlink appears on the navigation bar of the ICD Configuration web page only if you have purchased the Cisco IP ICD Enhanced or Cisco IP ICD Enhanced with CTI Option product.

Click the **Skills** hyperlink on the navigation bar of the ICD Configuration web page to access the Skills area of the ICD Configuration web page opens.

Use the Skills areas of the ICD Configuration web page to modify existing skills configuration or to create new skills.

Table 17-9 shows the tabular matter in the Skills area of the ICD Configuration web page.

Table 17-9   Skills Columns

Column Heading	Description
Skill Name	Customer-definable label that can be assigned to an agent.
Delete	Allows you to permanently remove the skill.

The main area of the Skills Configuration area of the ICD Configuration web page contains the following hyperlinks:

- **Add a New Skill**—Click this hyperlink to add a new skill.
- **Specific Skill Information**—Click a hyperlinked skill name to access the configuration information for that skill. On the page with the configuration information, you can click the Open Printable Report of this Skill Configuration to view a list of the resources associated with that skill.

Delete—Click the **Delete** icon to delete a skill.

This section contains the following topics:

- Adding a New Skill, page 17-13

Adding a New Skill

When you click the **Add a New Skill** hyperlink in the Skills area of the ICD Configuration web page, the Skills Configuration area opens.

Use the Skills Configuration area to add a new skill to an agent.

Table 17-10 shows the field in the Skills Configuration area of the ICD Configuration web page.

Table 17-10 Skill Configuration Area Field

Heading	Description
Skill Name	Customer-definable label for the skill.

Related Topic

- Creating, Modifying, and Deleting Skills, page 5-7

The Resources Hyperlink

Click the **Resources** hyperlink on the navigation bar of the ICD Configuration web page to assign a resource group and/or skills to a resource. The Resources area of the ICD Configuration web page opens.

Note An agent or supervisor must have an assigned ICD extension in order to appear in the list of resources in the Resources area of the ICD Configuration web page. (For information on assigning ICD extensions, see Provisioning the RM JTAPI Provider, page 5-3.)

Table 17-11 shows the tabular information displayed in the Resources area of the ICD Configuration web page.

Table 17-11 Resources Area Columns

Column Heading	Description
Resource Name	Name of the agent.
Resource Group	Resource group to which the agent has been assigned.
ICD Extension	ICD Extension assigned to the resource group.

The main area of the Resources area of the ICD Configuration web page contains the following hyperlink:

- **Specific Resource Information**—Click a hyperlinked resource or the information next to it to access resource configuration information.

- **Open Resources Summary Report hyperlink** Click this hyperlink to open the Resources Summary Report in a new window. For each resource, this report lists the resource groups associated with the resource, the ICD extension of the resource, and the number of CSQs to which the resource is assigned.

This section contains the following topics:

- Modifying a Resource, page 17-14

Modifying a Resource

When you click any of the hyperlinked information in the Resource area of the ICD Configuration web page, the Resource Configuration area opens.

Use the Resource Configuration area to modify resource configuration.

Table 17-12 shows the tabular information displayed in the Resources Configuration area of the ICD Configuration web page.

Table 17-12 Resource Configuration Area Columns

Field and Drop-Down Arrow Heading	Description
Resource Name	Name of the agent.
Resource ID	Unique identifying number of the agent.
ICD Extension	ICD Extension assigned to the resource group.
Resource Group	Resource group to which the agent has been assigned.
Automatic Available	If enabled, puts agents into Available State after the agent finishes a call and disconnects. **Note** If enabled, agents who want to enter the After Call Work State must manually place themselves into that state.
Assigned and Unassigned Skills List Box	Assigns and unassigns skills to an agent.
Competence Level (1-10)	Changes the competence level of an assigned skill (1 = Beginner, 10 = Expert).

This area also contains an **Open Printable Report of this Resource Configuration** hyperlink. Click this hyperlink to open a Resource Report for the resource. The Resource Report lists the resource's resource ID, resource name, ICD extension, resource group, automatic available status, skills, and CSQs.

Related Topic

- Assigning a Resource Group and Skills to an Individual Agent, page 5-10

The Resource Group Hyperlink

Click the **Resource Group** hyperlink on the navigation bar of the ICD Configuration web page to access the Resource Groups area of the ICD Configuration web page opens.

Use the Resource Groups area to display and modify the names of existing resource groups and to add new resource groups.

Table 17-13 shows the tabular information displayed in the Resource Groups area of the ICD Configuration web page.

Table 17-13 Resource Group Area Columns

Column Heading	Description
Resource Group Name	Contains the resource group name.
Delete	Permanently removes the resource group name.

The main area of the Resource Groups area of the ICD Configuration web page contains the following hyperlinks:

- **Add a New Resource Group**—Click this hyperlink to add a new resource group.
- **Specific Resource Group Information**—Click a hyperlinked resource group or the information next to it to access the configuration information for that resource group.
- **Delete**—Click the **Delete** icon to delete the resource group.

This section contains the following topics:

- Modifying a Resource Group Name, page 17-16
- Adding a New Resource Group, page 17-17

Modifying a Resource Group Name

When you click the hyperlinked name of any resource group in the Resource Groups area of the ICD Configuration web page, the Resource Groups Configuration area opens.

Use the Resource Configuration area to modify the name in the Resource Group Name field of the Resource Group Configuration area.

Table 17-14 shows the tabular information displayed in the Resource Group Configuration area of the ICD Configuration web page.

Table 17-14 Resource Group Configuration Area Field

Field	Description
Resource Group Name	Name of the resource group to which you want to assign agents.

The main area of the Resource Groups Configuration area of the ICD Configuration web page contains the following hyperlink:

- **Open Printable Report of this Resource Group Configuration**—Click this hyperlink to display a list of all available resources for this resource group.

Adding a New Resource Group

When you click the **Add a New Resource Group** hyperlink in the Resource Groups area of the ICD Configuration web page, the Resource Groups Configuration area opens.

Use the Resource Configuration area to enter the resource group name into the Resource Group Name field.

Related Topic

- Creating, Modifying, and Deleting Resource Groups, page 5-4

The Contact Service Queues Hyperlink

Click the **Contact Service Queue** hyperlink on the navigation bar of the ICD Configuration web page to access the Contact Service Queues area.

Use the Contact Service Queues area of the ICD Configuration web page to display existing CSQs, to delete a CSQ, and to add a new CSQ.

Table 17-15 shows the tabular information displayed in the Contact Service Queues area of the ICD Configuration web page.

Table 17-15 Contact Service Queues Area Columns

Column Heading	Description
Name	Name of the resource or skill group.
Contact Queuing Criteria	Algorithm used to order the queued calls (contacts).
Resource Pool Selection Model	The resource selection criteria chosen for this CSQ.
Resource Pool	The skills or resource group used for this CSQ.
Delete	Allows you to permanently remove the CSQ.

The main area of the Contact Service Queues area of the ICD Configuration web page contains the following hyperlinks:

- **Add a New Contact Service Queue**—Click this hyperlink to add a new CSQ.

- **Specific CSQ Information**—Click a hyperlinked CSQ or the information next to it to access the configuration information for that CSQ. On this configuration information page, click the **Open Printable Report of this CSQ Configuration** hyperlink to open the Contact Service Queue Report in a new window. For this CSQ, the report lists the contact service queue name, contact queuing criteria, automatic work status, resource selection criteria, resource pool selection model, resource group, and resources.

- **Delete**—Click the **Delete** icon to delete the CSQ.

This section contains the following topics:

- Adding a CSQ, page 17-19

Adding a CSQ

When you click the **Add a New Contact Service Queue** hyperlink in the Contact Service Queue area of the ICD Configuration web page, the Contact Service Queue Configuration area opens. Use the Contact Service Queue Configuration area to add a new CSQ.

Table 17-16 shows the fields in the Contact Service Queue Configuration area of the ICD Configuration web page.

Table 17-16   First Contact Service Queue Configuration Area Fields

Field Heading	Description
CSQ Name	The name of the CSQ.
Contact Queuing Criteria	Algorithm used to order the queued calls.
Automatic Work	Determines whether agents in this CSQ automatically move to Works state after a call. Options are Enabled and Disabled. Enabled causes the agent to go into Work state automatically when a call ends. Disabled causes the agent to enter Ready or Not Ready state when a call ends, depending on the Automatic Available setting for the agent.
Resource Pool Selection Model	Represents the resource groups or skills that will handle calls that select this CSQ.
Service Level	Target maximum time a call is queued before it is connected to an agent in this field.
Service Level Percentage	Target goal for percentage of contacts that meet the service level in this field.

After you complete the first page of the Contact Service Queue Configuration area, click **Next** to open the second Contact Service Queue Configuration page.

Table 17-17 shows the fields in the second Contact Service Queue Configuration area of the ICD Configuration web page.

Table 17-17 Second Contact Service Queue Configuration Area Fields

Field Heading	Description
Contact Service Queue Name	Name of the CSQ entered on the previous page.
Resource Selection Criteria (continued on next page)	Determines how agents are selected to handle calls. If Resource Groups are used for the Resource Selection Model, Resource Selection Criteria includes: • Longest Available—Selects the agent who has been in the Ready State for the longest amount of time. • Linear—Selects the next available agent with the highest priority. Priority is determined by the order of agents in the Show Resources list; the higher the agent in the list, the higher the agent's priority. • Circular—Selects next available agent with the highest priority, based on the last agent selected and the order of agents in the Show Resources list. • Most Handled Contacts—Selects the agent that has answered the most ICD calls. • Shortest Average Handle Time Model—Selects the agent with the smallest average call-handling time.

Table 17-17 Second Contact Service Queue Configuration Area Fields

Field Heading	Description
Resource Section Criteria, (continued)	If Resource Skills are used for the Resource Pool Selection Model, Resource Selection Criteria includes: • Longest Available — Selects the agent who has been in the Available state for the longest amount of time. • Most Handled Contacts — Selects the agent who has answered the most handled calls. • Shortest Average Handle Time — Selects the agent who generally spends the least amount of time talking to customers. • Most Skilled — Used for expert agent call distribution. Selects the agent with the highest competency level and who has been available for the longest amount of time. • Least Skilled — Used for expert agent call distribution. Selects the agent with the lowest competency level and who has been available for the longest amount of time.
Resource Group or Assigned Skills/Unassigned Skills	Determines which resource group or skills are assigned to this CSQ.
Competence Level (if selecting skills)	Determines the minimum competence level for the skills assigned to the CSQ
Show Resources	Click this button to view the list of agents meeting the criteria for the CSQ.

Related Topic

• Creating, Modifying, and Deleting Contact Service Queues, page 5-13

The RM JTAPI Provider Hyperlink

Click the **RM JTAPI Provider** hyperlink on the navigation bar of the ICD Configuration web page to return to the RM JTAPI Provider area of the ICD Configuration web page.

(The RM JTAPI Provider area automatically opens when you first choose **ICD** from the Subsystems menu of the CRA Administration menu bar.)

The Cisco IP ICD Resource Manager (RM) uses a JTAPI user configured in Cisco CallManager for monitoring agent phones, controlling agent states, and routing and queueing calls.

Use the RM JTAPI Provider area of the ICD Configuration web page to identify the JTAPI user you want the Resource Manager to use.

Table 17-18 describes the fields of the RM JTAPI Provider area of the ICD Configuration web page.

Table 17-18 RM JTAPI Provider Area Fields

Field	Description
RM JTAPI Provider	IP address or host name of the Cisco Media Convergence Server (MCS) running Cisco CallManager CTI Manager. **Note** You can enter up to two CTI Managers, separated by a space. If the first CTI Manager becomes unavailable, the second one connects and maintains calls.
User ID	User ID of the Cisco CallManager.
Password	Password that you defined for the User ID.

Related Topic

• Provisioning the RM JTAPI Provider, page 5-3

The Assign Skills Hyperlink

> **Note** The **Assign Skills** hyperlink appears on the navigation bar of the ICD
> Configuration web page only if you have purchased the Cisco IP ICD Enhanced
> or Cisco IP ICD Enhanced with CTI Option product.

Click the **Assign Skills** hyperlink on the navigation bar of the ICD Configuration
web page to access the Assign Skills area of the ICD Configuration web page.

Use the Assign Skills areas of the ICD Configuration web page to modify an
existing resource group and skills configuration or to assign new resource groups
and skills to the selected agents.

Table 17-19 shows the tabular information in the Assign Skills area of the ICD
Configuration web page.

Table 17-19 Assign Skills Columns

Column Heading	Description
Resource Name	Contains the agent's name.
Resource Group	Contains the resource group assigned to the agent.
ICD Extension	Contains the ICD extension of the agent.

This section contains the following buttons:

- **Add Skill**—Click the Add Skills button to add new skills or resource groups
  to the selected agents.
- **Remove Skill**—Click the Remove Skills button to remove skills from the
  selected agents.

This section contains the following topics:

Adding Skills

When you click the **Add Skill** button in the Assign Skills area of the ICD Configuration web page, the Add Skills area opens. Use the Add Skill area to add a resource group and skills to the selected agents.

Table 17-20 shows the fields in the Add Skill area of the ICD Configuration web page.

Table 17-20 Add Skill Area Fields

Field Heading	Description
Resource Group	List of the available resource groups.
Skills to Add	List of skills to be added to the selected agents.
Skills	List of the available skills.
Competence Level	Competence level of the agents in the selected skill.

Table 17-21 shows the buttons in the Add Skill area of the ICD Configuration web page.

Table 17-21 Add Skill Area Buttons

Button	Description
Update	Applies the changes.
Cancel	Cancels the changes.

Related Topic

•   Assigning Resource Groups and Skills to Agents in Bulk, page 5-11

Removing Skills

When you click the **Remove Skill** button in the Assign Skills area of the ICD Configuration web page, the Remove Skill area opens. Use the Remove Skill area to remove skills from the selected agents.

Table 17-22 shows the fields in the Remove Skill area of the ICD Configuration web page.

Table 17-22 Remove Skill Area Fields

Field Heading	Description
Skills to Remove	List of skills that can be removed from the selected agents.
Skills	List of the skills not assigned to the agents.

Table 17-23 shows the buttons in the Remove Skill area of the ICD Configuration web page.

Table 17-23 Remove Skill Area Buttons

Button	Description
Update	Applies the changes.
Cancel	Cancels the changes.

Related Topic

- Removing Skills from Agents in Bulk, page 5-12

The ICM Menu Option

The Cisco CRA system uses the ICM (Intelligent Contact Manager) subsystem of the CRA Engine to communicate with Cisco ICM software to direct calls to other systems such as interactive voice response units (VRUs) and ACD systems, as part of the Cisco IP Contact Center (IPCC) solution.

Choose **Subsystems > ICM** from the CRA Administration menu bar to configure the ICM subsystem. The ICM Configuration web page opens.

Use the areas of the ICM Configuration web page to add or modify ICM configuration parameters and to modify VRU script information.

The ICM Configuration navigation bar contains the following hyperlinks:

- **General**—Click this hyperlink to add or modify ICM configuration parameters.

- **ICM VRU Scripts**—Click this hyperlink to modify VRU script information.

This section contains the following topics:

The General Hyperlink

Click the **General** hyperlink to return to the General area from any other area of the ICM Configuration web page.

(The General area automatically opens in the ICM Configuration web page when you first choose the **ICM** menu option from the Subsystems menu.)

Use the General area of the ICM Configuration page to add or modify ICM configuration parameters.

Table 17-24 shows the tabular information in the General area of the ICM Configuration web page.

Table 17-24 ICM Configuration Columns

Column Heading	Description
VRU Connection Port	Specifies the TCP/IP socket number used for receiving messages from the Cisco ICM system.
	Note You can copy the VRU Connection Port value from VRU PIM configuration dialog box of the VRU peripheral gateway (PG) machine. (Default value: 5000.)
Service Control	Enables and disables the service control interface. You must enable the service control interface to use the ICM subsystem.

Table 17-24 ICM Configuration Columns (continued)

Column Heading	Description
Parameter Separator	Delineates individual parameters in a multiple parameter variable.
Additional VRU Call Information	Specifies which of the listed expanded call variables to use to pass additional call-related information.

Related Topic

The ICM VRU Scripts Hyperlink

Click the **ICM VRU Scripts** hyperlink on the navigation bar of the ICM Configuration web page to access the first ICM VRU Scripts area opens.

Cisco IPCC uses ICM Voice Response Unit (VRU) scripts to handle interactions with contacts. These scripts are loaded as applications on the CRA Engine.

Use the first ICM VRU Scripts area of the ICM Configuration web page to modify VRU script information.

Table 17-25 shows the tabular information displayed in the first ICM VRU Scripts area of the ICM Configuration web page.

Table 17-25 ICM VRU Scripts Columns

Column Heading	Description
VRU Script Name	Displays the VRU script name.
Script	Displays the actual script that corresponds to the CRA script name.
Delete	Permanently removes a VRU script.
Reload	Reloads a VRU script.

The main area of the first ICM VRU Scripts area of the ICM Configuration web page contains the following hyperlinks:

- **Add a New VRU Script**—Click this hyperlink to add a new VRU script.
- **Specific VRU Script Information**—Click a hyperlinked VRU Script or the information next to it to access the configuration information of the VRU script.
- **Delete**—Click the **Delete** icon to delete the VRU script.
- **Reload**—Click the **Reload** icon to reload the previous version of a VRU script.

This section contains the following sections:

Modifying ICM VRU Scripts

When you click the **Add a New VRU Script** hyperlink in the first VRU Scripts area of the ICM Configuration web page, the second ICM VRU Scripts area opens.

Use the second ICM VRU Scripts area to modify ICM VRU script configuration.

Table 17-26 shows the tabular information in the second ICM VRU Scripts area of the ICM Configuration web page.

Table 17-26 ICM VRU Scripts Fields

Fields	Description
VRU Script Name	VRU script name you want to add.
Script	CRA script associated with the VRU script.

Adding an ICM VRU Script

When you click the **Add a New VRU Script** hyperlink in the first VRU Scripts area of the ICM Configuration web page, the second ICM VRU Scripts area opens.

Use the second ICM VRU Scripts area to add an ICM VRU script.

Related Topic

- Configuring ICM VRU Scripts, page 6-6

The Database Menu Option

The Cisco CRA system uses the Database subsystem of the CRA Engine to communicate with database servers, in order to obtain information to relay to callers or to make application decisions. The Database subsystem enables the CRA applications to obtain information from datasources, which are databases configured to communicate with the CRA system.

Note The Database subsystem does not support database views, nor can this Database subsystem execute store procedures.

Choose **Subsystems > Database** from the CRA Administration menu bar to configure the Database subsystem. The first Enterprise Database Subsystem Configuration web page opens.

Use the first Enterprise Database Subsystem Configuration web page to display existing datasources, modify or delete existing datasources, or to add a new datasource.

Table 17-27 shows the tabular information displayed in the first Enterprise Database System Configuration area.

Table 17-27 Enterprise Database Subsystem Configuration Web Page Columns

Column Heading	Description
Data Source Name	Datasource name configured when an ODBC[1] datasource is defined.
Username	Username defined for connecting to the enterprise database.
Password	Password defined for connecting to the enterprise database.
Maximum Number of Connections	Maximum number of connections allowed to connect to the database.

1.   ODBC = Open Database Connectivity

The first Enterprise Database Subsystem Configuration web page contains the following hyperlinks:

- **Add a New Datasource**—Click this hyperlink to add a new datasource.

- **Specific Datasource Information**—Click a hyperlinked datasource or the information next to it to access datasource configuration information.

- **Delete**—Click the **Delete** icon to delete a datasource.

This section contains the following topic:

- The Add a New Datasource Hyperlink, page 17-31

The Add a New Datasource Hyperlink

Click the **Add New Data Source** hyperlink in the first Enterprise Database Subsystem Configuration area to add a new datasource. The second Enterprise Database Subsystem Configuration area opens.

Use the second Enterprise Database Subsystem Configuration area to add a new datasource.

Table 17-28 shows the tabular information displayed in the second Enterprise Database Subsystem Configuration area.

Table 17-28 Second Enterprise Database Subsystem Configuration Fields

Heading	Description
Data Source Name	Data Source Name configured when an ODBC Data Source is defined in this field.
Username	Username defined for connecting to the enterprise database in this field.
Password	Password defined for connecting to the enterprise database.
Maximum Number of Connections	Maximum number of connections allowed to connect to the database.

Related Topic

• Provision the Database Subsystem, page 6-10

The HTTP Menu Option

The Cisco CRA system uses the HTTP subsystem of the CRA Engine to add components to the CRA Engine that allow applications to be triggered in response to requests from a variety of web clients, including computers and IP phones.

Choose **Subsystems > HTTP** from the CRA Administration menu bar to configure the HTTP subsystem. The first HTTP Trigger Configuration web page opens.

Use the first HTTP Trigger Configuration web page to display, modify, and delete existing HTTP triggers, and to add new HTTP triggers.

Table 17-29 shows the tabular information displayed in the first HTTP Trigger Configuration area.

Table 17-29 First HTTP Trigger Configuration Web Page Columns

Column Heading	Description
URL	URL that associated with the HTTP application.
Application	HTTP application name.
Session	Maximum instances of the application that can be simultaneously running when triggered by this particular HTTP trigger.
Enabled	If true, the trigger is enabled; if false, the trigger is disabled.
Copy	Allows you to copy an existing HTTP application. **Note** When you click the Copy button, the second HTTP Trigger Configuration are opens, displaying the copied configuration so that you can make changes if desired.
Delete	Allows you to delete an HTTP trigger.
Reload	Allows you to reload the HTTP trigger.

The first Enterprise Database Subsystem Configuration web page contains the following hyperlinks:

- **Add a New HTTP Trigger**—Click this hyperlink to add a new HTTP trigger.

- **Specific HTTP Trigger Information**—Click a hyperlinked HTTP Trigger or the information next to it to access the configuration information for that HTTP trigger.

- **Copy**—Click the **Copy** icon to copy the configuration information of an HTTP trigger.

- **Delete**—Click the **Delete** icon to delete an HTTP trigger.

- **Reload**—Click the **Reload** icon to delete an HTTP trigger.

The Add a New HTTP Trigger Hyperlink

Click the **Add New HTTP Trigger** hyperlink in the first HTTP Trigger Configuration web page to add a new HTTP trigger. The second HTTP Trigger Configuration web page opens.

Use the second HTTP Trigger Configuration web page to add a new HTTP trigger to an application.

Table 17-30 shows the tabular information displayed in the second HTTP Trigger Configuration area.

Table 17-30 Second HTTP Trigger Configuration Web Page Fields

Field Heading	Description
URL	URL that will be associated with the HTTP application. **Note** The URL must be entered as */myapp*, where *myapp* is the URL of the application. The URL can not contain any spaces, special characters, or backslashes.
Language	Default language to be associated with the incoming HTTP request contact.
Application Name	Name of the application.
Maximum Number Of Sessions	Maximum instances of the application that can run simultaneously when triggered by this particular HTTP trigger.
Idle Timeout (in ms)	Maximum amount of "wait time" before the CRA system rejects the HTTP request for this trigger.
Enabled	Enables or disables the trigger.

Related Topic

The eMail Menu Option

The Cisco CRA system uses the eMail subsystem of the CRA Engine to communicate with your e-mail server and enable your applications to create and send email.

Choose **Subsystems > eMail** from the CRA Administration menu bar to configure the eMail subsystem. The eMail Configuration web page opens.

Use the eMail Configuration web page to configure e-mail functionality so that CRA scripts created with the e-mail steps will function correctly.

The e-mail configuration identifies the default e-mail address and server to be used for sending e-mail (including e-pages and faxes) and for receiving acknowledgments.

If your e-mail system is configured to receive acknowledgments, you should process the mailbox you identify in your configuration to determine whether or not e-mail was successfully sent.

Table 17-31 shows the tabular information displayed on the eMail Configuration web page.

Table 17-31 eMail Configuration Fields

Heading	Description
Mail Server	Location of the e-mail server.
eMail Address	Return e-mail address.

Related Topic

• Provision the eMail Subsystem, page 6-13

The Cisco Media Menu Option

The Cisco CRA system uses the Media subsystem of the CRA Engine to configure Cisco Media Termination (CMT) dialog groups that can be used to handle simple Dual-Tone Multi-Frequency (DTMF) based dialog interactions with customers. A dialog group is a pool of dialog channels in which each channel is used to perform dialog interactions with a caller.

Choose **Subsystems > Cisco Media** from the CRA Administration menu bar to configure dialog groups. The first Cisco Media Termination Dialog Group Configuration web page opens.

Use the first Cisco Media Termination Dialog Group Configuration web page to modify existing CMT dialog groups and to add new dialog groups.

Table 17-32 shows the tabular information displayed in the first Cisco Media Termination Dialog Group Configuration area.

Table 17-32 First Cisco Media Termination Dialog Group Configuration Columns

Column Heading	Description
GroupID	Group ID associated with the media.
Description	CMT group description.
Channels	Number of channels associated with the group.
Copy	Allows you to copy an existing CMT dialog group.
	Note When you click the **Copy** icon, the second Cisco Media Termination Dialog Group Configuration area opens, displaying the copied configuration so that you can make changes, if desired.
Delete	Allows you to delete a CMT dialog group.
Reload	Allows you to reload a CMT dialog group.

The first Cisco Media Termination Dialog Group Configuration web page contains the following hyperlinks:

- **Add a New CMT Dialog Control Group**—Click this hyperlink to add a new CMT dialog control group.

- **Specific CMT Dialog Control Group Information**—Click a hyperlinked CMT dialog control group or the information next to it to access configuration information.

- **Copy**—Click the **Copy** icon to copy the configuration information of a CMT dialog control group.

- **Delete**—Click the **Delete** icon to delete a CMT dialog control group.
- **Reload**—Click the **Reload** icon to reload the configuration information for a CMT dialog control group.

This section contains the following topic:

The Add a New Dialog Control Group Hyperlink

Click the **Add** a **New Dialog Control Group** hyperlink in the first Cisco Media Termination Dialog Group Configuration web page to add a new CMT dialog group. The second Cisco Media Termination Dialog Group Configuration web page opens.

Use the second Cisco Media Termination Dialog Group Configuration web page to add a new CMT dialog group.

Table 17-33 describes the fields in the second Cisco Media Termination Dialog Group Configuration web page.

Table 17-33 Second Cisco Media Termination Dialog Group Configuration Web Page Fields

Heading	Description
Group ID	Group ID for this CMT dialog group.
Description	Description for this CMT dialog group.
Number Of Licensed IVR Ports	*Display only.* Number of licensed IVR ports.
Maximum Number Of Channels	Maximum number of channels associated with this group. **Note** You can specify any value for Maximum Number Of Channels, but restrictions are placed on the system when a call is made. This restriction is imposed by the number of licensed IVR ports on your system.

Related Topic

The Nuance ASR Menu Option

The Cisco CRA system uses the Nuance ASR (Automatic Speech Recognition) subsystem of the CRA Engine to allow users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone.

Choose **Subsystems > Nuance ASR** from the CRA Administration menu bar to configure the Nuance ASR subsystem. The first area of the Nuance ASR Configuration web page opens.

Use the areas of the Nuance ASR Configuration web page to modify existing dialog control groups or to add new dialog groups.

The Nuance ASR Configuration navigation bar contains the following hyperlinks:

- **Nuance ASR Configuration**—Choose this option to configure your speech server.

- **Nuance ASR Dialog Control Groups**—Choose this option to configure Nuance ASR dialog control groups.

This section contains the following topics:

The Nuance ASR Configuration Hyperlink

Click the **Nuance ASR Configuration** hyperlink on the navigation bar of the Nuance ASR Configuration web page to return to the first Nuance ASR Configuration web page.

(The Nuance ASR Configuration web page automatically opens when you first choose **Nuance ASR** from the Subsystems menu of the CRA Administration menu bar.)

Use the first Nuance ASR Configuration web page to configure your speech server.

Table 17-34 shows the tabular information displayed in the first Nuance ASR Configuration web page.

Table 17-34 First Nuance ASR Configuration Web Page Options

Field or Drop-Down Arrow Headings	Description
Speech Server Host Name(s)	Location of one or more speech servers (separated by spaces or a comma).
Refresh Frequency	One of the following refresh frequency rates: • Never • Once • Daily • Weekly **Note** The Refresh Frequency option determines how frequently the refresh task will be run. When the system runs a refresh, the Refresh Task reads the names, extensions and other information from the Cisco CallManager User Directory into a form that can be used for the recognition of spoken names, by the Name to User step.
Refresh Start Task Time	Start time to refresh all usernames from the Cisco CallManager User Directory.

The first Nuance ASR Configuration web page contains the following hyperlink:

• **Start Refresh Task Now**—Click this hyperlink to start the refresh task.

The Refresh task reads the user names and extensions from the Cisco CallManager directory and compiles them into a recognition package that is used by the Name to User step when associated with a Nuance ASR dialog channel. (For more information on the Name to User step, refer to the *Cisco Customer Response Application Editor Step Reference Guide*.)

If you modify the users in the Cisco CallManager directory (add, change, or delete), you must run the Refresh task again or the changes will not be reflected in the recognition results from the Name to User step.

You have three options:

- Never run the Refresh task. This is an acceptable option, as long as no application uses the Name-To-User step in ASR mode.

- Let the scheduler automatically run once, once a day, or once a week at a configured time (preferably after peak hours).

- Run the Refresh task on demand, using the **Start Refresh Task Now** hyperlink from the Nuance ASR Configuration web page.

The Nuance ASR Dialog Control Groups Hyperlink

Click the **Nuance ASR Dialog Control Groups** hyperlink on the navigation bar of the Nuance ASR Configuration web page to access the second Nuance ASR Configuration web page opens.

Table 17-35 shows the tabular information displayed in the second Nuance ASR Configuration area.

Table 17-35 Second Nuance ASR Configuration Area Columns

Column Heading	Description
Group ID	Associated group ID.
Description	Description of this Nuance dialog group.
Max Number of Sessions	Maximum number of calls that can be processed simultaneously by this group.
Delete	Allows you to delete a Nuance ASR dialog group.
Reload	Allows you to reload a Nuance ASR dialog group.

Table 17-36 describes the button in the second Nuance ASR Configuration area.

Table 17-36 Second Nuance ASR Configuration Area Button

Name	Description
Reload	Reloads all Nuance ASR dialog groups.

The second Nuance ASR Configuration web page contains the following hyperlinks:

- **Add a New Nuance ASR Dialog Control Group**—Click this hyperlink to add a new Nuance ASR dialog control group.
- **Specific Nuance ASR Dialog Control Group Information**—Click a hyperlinked Nuance ASR dialog control group or the information next to it to access configuration information for that Nuance ASR dialog control group.
- **Delete**—Click the **Delete** icon to delete a Nuance ASR dialog control group.
- **Reload**—Click the **Reload** icon next to delete a Nuance ASR dialog control group.

This section contains the following topics:

- The Add a New ASR Dialog Control Group Hyperlink, page 17-40

The Add a New ASR Dialog Control Group Hyperlink

Click the **Add** a **New ASR Dialog Control Group** hyperlink in the second Cisco Nuance ASR Configuration web page to add a new ASR dialog group. The Cisco Nuance ASR Dialog Control Groups web page opens.

Table 17-37 describes the fields in the Nuance ASR Dialog Control Groups web page.

Table 17-37 Nuance ASR Dialog Control Group Web Page Fields

Field Heading	Description
Group ID	Group ID for this Nuance ASR dialog group.
Description	Description of this Nuance ASR dialog group.

Table 17-37 Nuance ASR Dialog Control Group Web Page Fields (continued)

Field Heading	Description
Number Of Licensed IVR Ports	*Display only.* Number of licensed IVR ports.
Maximum Number Of Channels	Maximum number of channels associated with this dialog group. **Note** You can assign any value for Maximum Number Of Channels, but restrictions are placed on the system when a call is made. This restriction is imposed by the number of licensed IVR ports on your system.

Related Topic

The Nuance TTS Menu Option

The Cisco CRA system uses the Nuance TTS (Text-to-Speech) subsystem of the CRA Engine to convert plain text (UNICODE) into spoken words in order to provide a user with information or to prompt a user to respond to an action.

Choose **Subsystems > Nuance TTS** from the CRA Administration menu bar to configure the Nuance TTS subsystem. The first Nuance TTS Server Configuration web page opens.

Use the Nuance TTS Server Configuration web pages to modify existing Nuance TTS server information and to add new Nuance TTS servers.

Table 17-38 shows the tabular information displayed in the first Nuance TTS Server Configuration area.

Table 17-38 First Nuance TTS Server Configuration Area Columns

Column Heading	Description
id	Unique identifier for the TTS server.
Server Host	Host name or IP address of the TTS server.

Table 17-38 First Nuance TTS Server Configuration Area Columns (continued)

Column Heading	Description
port	TCP[1] port number used to open a TTS connection to the TTS server. **Note** The range is between 30000 and 32323.
Language	Language supported by the server.
Gender	Gender supported by the server.
Delete	Allows you to permanently remove a TTS server.

1. TCP = Transmission Control Protocol

The main area of the first Nuance TTS Server Configuration web page contains the following hyperlinks:

- **Add New Nuance TTS Server**—Click this hyperlink to add a new Nuance TTS server.

- **Specific Nuance TTS Server Information**—Click a hyperlinked Nuance TTS server or the information next to it to access the configuration information for the Nuance TTS server.

- **Delete**—Click the **Delete** icon to delete a Nuance TTS server.

This section contains the following topic:

-

The Add a Nuance TTS Server Hyperlink

Use the second Nuance TTS Server Configuration area to add a new Nuance TTS server.

Click the **Add New Nuance TTS Server** hyperlink in the first Nuance TTS Server Configuration area to add a new Nuance TTS server. The second Nuance TTS Server Configuration area opens.

Table 17-39 shows the tabular information displayed in the second Nuance TTS Server Configuration web page.

Table 17-39 Second Nuance TTS Server Configuration Fields

Field Heading	Description
Id	Unique identifier of the TTS server.
TTS Server Host	Host name or IP address of the TTS server.
TTS Port	TCP port number (the port number that is used to open a TTS connection to the TTS server). **Note** The range is between 30000 and 32323.
TTS Language	Language in which the text will be played back.
Voice Gender	Gender of the voice that will speak the text.

Related Topic

• Provision the Nuance TTS Subsystem, page 4-12

The Tools Menu

The Tools menu of the Cisco Customer Response Applications (CRA) Administration web interface provides access to system tools.

Use the Tools menu to perform a wide variety of administrative tasks.

The Tools menu contains the following menu options:

- **Alarm Definition**—Choose this option to use the alarm catalog to find information about an alarm message name.

- **Plug-ins**—Choose this option to download plug-ins that you can use to enhance the CRA Engine.

- **Real-time Reporting**—Choose this option to generate reports that provide detailed information about the status of your CRA system.

- **Real-time Snapshot Config**—Choose this option to configure the CRA database connection to a wallboard display.

- **Historical Reporting**—Choose this option to perform Historical Reporting tasks, including configuring the database server, synchronizing data, configuring users, installing client software, and purging your database.

- **Prompt Management**—Choose this option to display, modify, or delete existing prompts and to add new prompts.

- **Spoken Name Upload**—Choose this option to upload .wav files of the spoken names of users, so that CRA applications can uses the .wav files as part of prompts.

- **User Maintenance**—Choose this option to assign access levels to administrators and supervisors.

- **Troubleshooting Tips**—Choose this option to search the troubleshooting database for suggestions on how to solve problems that may arise in the performance of your CRA system.

This chapter includes the following sections:

The Alarm Definition Menu Option

The Cisco CRA Engine maintains a list of alarm catalogs, each of which contains a list of alarms and alarm definitions. Each alarm definition includes the alarm name, a description, an explanation, recommended actions, and related information.

Use the Alarm Definitions web page to find information about an alarm message name.

Choose **Tools > Alarm Definition** from the CRA Administration menu bar to search for alarm definitions. The Alarm Definitions web page opens. (See Figure 18-1).

Figure 18-1   Alarm Definitions Web Page

Table 18-1 describes the fields of the Alarm Definitions web page.

Table 18-1   Alarm Definitions Web Page Options

Field or Drop-Down Menu Heading	Description
Catalog	Catalog of alarm message names.
Enter Alarm Name	Alarm message name for which you want to locate a stored alarm file.

Table 18-2 describes the button on the Alarm Definitions web page.

Table 18-2   Alarm Definitions Web Page Button

Button	Description
Search	Click to locate the stored alarm file.

For more information on Alarms and Alarm definitions, please see the *Cisco Customer Response Applications Serviceability Guide*.

The Plug-ins Menu Option

The CRA system employs software components called *plug-ins* that you can use to enhance the CRA Engine.

Choose **Tools > Plug-ins** from the CRA Administration menu bar to display a list of these plug-ins. The Plug-ins web page opens. (See Figure 18-2.)

Use the Plug-ins web page to download plug-ins.

Figure 18-2   Plug-ins Web Page

The Plug-ins web page contains one or more of the following hyperlinks (depending on the Cisco CRA package you have purchased):

- **Cisco CRA Editor**—Click this hyperlink to install the client-side Cisco CRA Editor. For more information, see the *Cisco Customer Response Applications Developer Guide*.

- **Cisco Desktop Product Suite**—Click this hyperlink to install Cisco Desktop Administrator, Supervisor Desktop, or Agent Desktop. For more information, see *Cisco Customer Response Applications Supervisor Desktop Plug-in Tasks* and *Cisco Customer Response Applications Agent Desktop Plug-in Tasks*.

- **Cisco CRA Historical Reports**—Click this hyperlink to install client-side historical reporting. For more information, see *Cisco Customer Response Applications Historical Reports User Guide*.

> **Note**   If you will use Cisco Historical Reporting, the Cisco CRA Historical Reports client system must be same version as the CRA system.

- **Cisco CRA SDK**—Click this hyperlink to install Cisco CRA SDK.

The Real-time Reporting Menu Option

The Real-time Reporting tool is a Java applet that you can use to generate a variety of reports that provide detailed information about the status of your CRA system.

Choose **Tools > Real Time Reporting** from the CRA Administration menu bar to generate real-time reports. The Application Reporting web page opens. (See Figure 18-3.)

Use the Application Reporting web page to access the Real-time Reporting tool.

Figure 18-3   Application Reporting Web Page

Note Real-time Reporting requires the Java plug-in. If the Java plug-in is not already installed on the PC on which you are viewing the reports, the CRA system will automatically install it when you choose **Tools > Real Time Reporting**.

The Application Reporting web page is a stand-alone component of the CRA Administration interface. It has its own menu bar, which replaces the CRA Administration menu bar.

The Application Reporting menu bar contains the following menu options:

- **Report**—Choose this option to display a list of available top-level reports.
- **Tools**—Choose this option to reset all the statistics and to display a report that is optimized for printing.

- **Views**—Choose this option to specify which view of reports you receive.

- **Settings**—Choose this option to set the look and feel of the Real-time Reporting client, set the polling (refresh) interval times, and set the amount of times the server will attempt to reconnect.

- **Help**—Choose this option to display system information and to access Cisco CRA online help.

This section contains the following topics:

The Report Menu

The Report menu gives you access to a variety of top-level reports:

Note All real-time reports display a "Last Updated At" field, which indicates the time of the snapshot. All summary reports display both a start time (which indicates when the summary statistics started being collected) and the current time.

This section contains the following topics:

The Contacts Summary Menu Option

Choose **Reports > Contacts Summary** from the Application Reporting menu bar to access the Contacts Summary web page. (See Figure 18-4.)

Use the Contacts Summary web page to view specific contact information for call contacts, e-mail contacts, HTTP contacts, and total number of contacts.

Figure 18-4   Contacts Summary Web Page

Table 18-3 describes the information provided on the Contacts Summary web page.

Table 18-3   Contact Summary Web Page Rows

Row Heading	Description
Active	Active contacts that are currently running.
Inbound	Number of inbound contacts since the statistics were last reset.
Outbound	Number of outbound contacts since the statistics were last reset.
Connected	Number of connected contacts since the statistics were last reset.
	This row reports contacts that are connected to resources (for example, a call connected to an ACD[1] agent).
Terminated	Number of terminated contacts since the statistics were last reset.
	This row reports contacts that are ended normally by the application (for example, a caller hangs up and the application terminates).
Rejected	Number of rejected contacts since the statistics were last reset.
	This row reports contacts that are not accepted and/or processed (as a result, for example, of insufficient resources or the rejection of the contact based on some customer-defined logic).
Aborted	Number of aborted contacts since the statistics were last reset.
	This row reports contacts improperly ended by a task associated with the application (as when, for example, the system generates an exception or can not invoke the application because of some error in the application).

Table 18-3   Contact Summary Web Page Rows (continued)

Row Heading	Description
Handled	Number of handled contacts since the statistics were last reset.
	This row reports contacts that are explicitly marked "Handled" by the application (typically when the application connects the contact to an ICD[2] agent).
Abandoned	Number of abandoned contacts since the statistics were last reset.
	This row reports contacts that end without being marked "Handled" by the application.
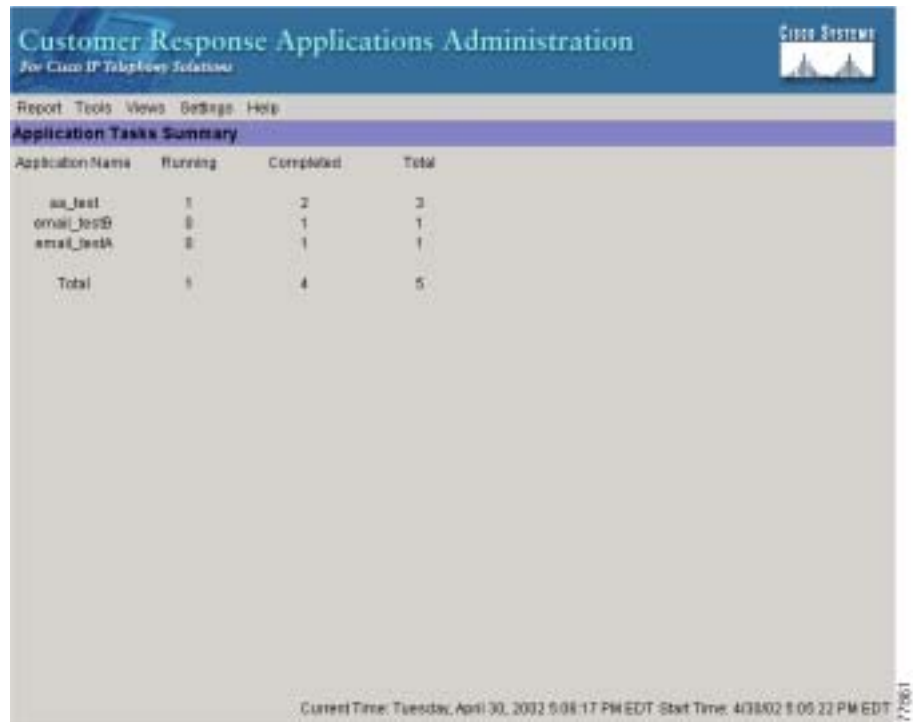
1.   ACD = Automatic Contact Distribution

2.   ICD = Integrated Contact Distribution

The Application Tasks Summary Menu Option

Choose **Reports > Application Tasks Summary** from the Application Reporting menu bar to access the Application Tasks Summary web page. (See Figure 18-5.)

Use the Application Tasks Summary web page to displays statistics that summarize the activity of specific applications.

Figure 18-5   Application Tasks Summary Web Page

Table 18-4 describes the information provided on the Application Tasks Summary web page.

Table 18-4   Applications Tasks Summary Web Page Columns

Column Heading	Description
Application Name	Names of the applications that are running or have run.
Running	Currently running applications.
Completed	Applications that have stopped running.
Total	Number of times a given application was invoked since the statistics were last reset.

The Application Tasks Menu Option

Choose **Reports > Application Tasks** from the Application Reporting menu bar to access the Application Tasks web page. (See Figure 18-6.)

Use the Application Tasks web page to view information about currently active applications.

Figure 18-6   Application Tasks Web Page
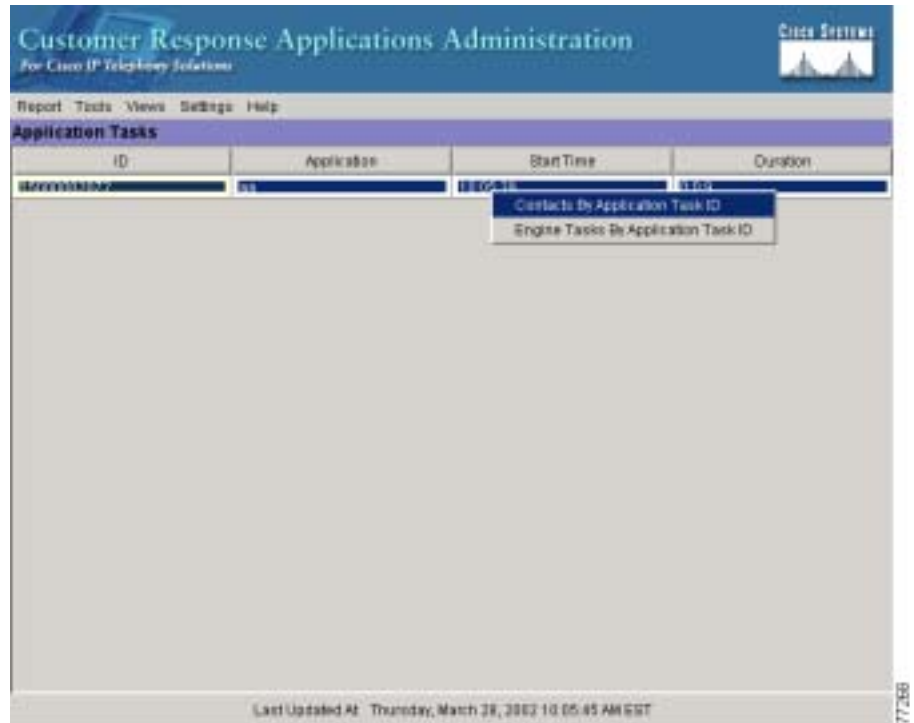
Table 18-5 describes the information provided on the Application Tasks web page.

Table 18-5   Application Tasks Web Page Columns

Column Heading	Description
ID	Unique application task ID.
Application	Name of the application.
Start Time	Time when the application task started.
Duration	Length of time that the application has been active.

Note If this report indicates that an application is running for a unusually long time, there may be a problem with the application. The application's script may not include error handling that prevents infinite retries if a call is longer present. If the application does not receive a disconnect signal after a call, the application repeatedly retries to locate the call, and causes the application to run for an unusually long time. To prevent this problem, include the proper error handling in the application script.

The Engine Tasks Menu Option

Choose **Reports > Engine Tasks** from the Application Reporting menu bar to access the Engine Tasks web page. (See Figure 18-7.)

Use the Engine Tasks web page to view information about currently active Engine tasks.

Figure 18-7   Engine Tasks Web Page

Table 18-6 describes the information provided on the Engine Tasks web page.

Table 18-6   Engine Tasks Web Page Columns

Column Heading	Description
ID	Unique identifier of the engine task.
	If the engine task is the main task running the application and the parent ID is empty, its identifier will match the Application Task Identifier.
Parent ID	ID of the parent of the engine task (if any).
Script	Name of the script that is running the task (if the task is running a Cisco CRA script).

Table 18-6   Engine Tasks Web Page Columns (continued)

Column Heading	Description
Start Time	Time that the task started.
Duration	Length of time the task has been active.

The Contacts Menu Option

Choose **Reports > Contacts** from the Application Reporting menu bar to access the Contacts web page. (See Figure 18-8.)

Use the Contacts web page to view information for all the active contacts.

Figure 18-8   Contacts Web Page

Table 18-7 describes the information provided on the Contacts web page.

Table 18-7   Contacts Web Page Columns

Column Heading	Description
Contact ID	Unique identifier used to represent this contact in this CRA server.
Contact Type	Type of contact: CallContact, EmailContact, or HttpContact.
Impl ID	Unique identifier provided by the particular type of contact. For example, for a call contact, this identifier would represent the Call Manager global call ID.
Start Time	Time stamp when the contact was created.
Duration	Length of time that the contact has been active.
Handled	If True, the contact has been handled; if False, the contact has not been handled.
Aborting	If True, the contact is being aborted with a default treatment; if False, the contact is not being aborted.
Application	Name of the application currently managing the contact.
Task	ID of the application task that is currently responsible for the contact.
Session	ID of the session currently managing the contact (if any).

You can access detailed information about specific contacts listed on the Contacts web page by performing one of the following procedures:

- Accessing Detailed Call Contact Information, page 18-17
- Accessing Detailed E-mail Contact Information, page 18-19
- Accessing Detailed HTTP Contact Information, page 18-20

Note The information displayed is dependent on the type of contact selected. Depending on the type of call, some fields may not be supported and will appear blank.

Accessing Detailed Call Contact Information

Right-click a specific call contact record in the Contacts web page to access the Call Contacts Detailed Info web page, which displays information for that specific record. (See Figure 18-9.)

Use the Call Contacts Detailed Info web page to view all information related to the call contact.

Figure 18-9   Call Contacts Detailed Info Web Page
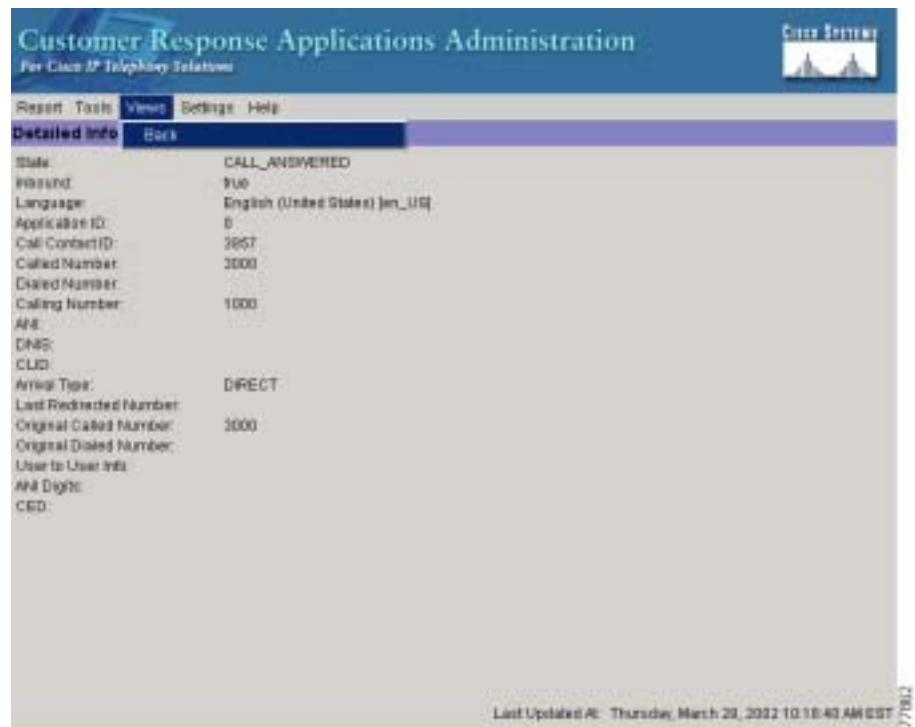
Table 18-8 describes the information provided on the Call Contacts Detailed Info web page.

Table 18-8   Call Contacts Detailed Info Web Page Rows

Heading	Description
State	Current state of the contact.
Inbound	If True, this call was received by the CRA server; if False, this call was placed as an outbound call by an application.
Language	The selected language context of the call.
Application ID	ID of the associated application.
Called Number	Called number for this call leg from the perspective of the called party.
Dialed Number	Dialed number for this call leg from the perspective of the calling party.
Calling Number	Calling number of the originator of this call.
ANI	Automatic number identification.
DNS	Dialed number identification service.
CLID	Caller ID.
Arrival Type	Information on how the call contact arrived in the system.
Last Redirected Number	Number from which the last call diversion or transfer was invoked.
Original Called Number	Originally called number.
Original Dialed Number	Originally dialed number.
ANI Digits	Automatic Number Identification information indicator digit codes.
CED	Entered digits that were gathered by the network before the call was received. Note Calls running ICM applications are also reported here.

Accessing Detailed E-mail Contact Information

Right-click a specific e-mail contact record in the Contacts web page to access the Email Detailed Info web page, which displays information for that specific record. (See Figure 18-10.)

Use the Email Detailed Info web page to view all information related to the e-mail contact.

Figure 18-10 Email Detailed Info Web Page
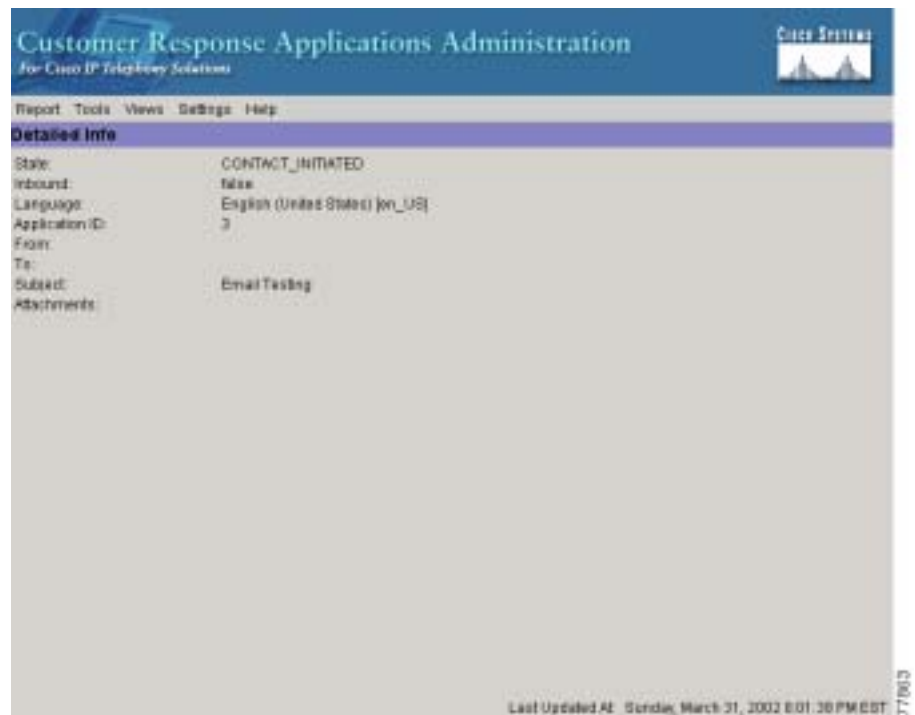
Table 18-9 describes the information provided on the Email Detailed Info web page.

Table 18-9   Email Detailed Info Web Page Rows
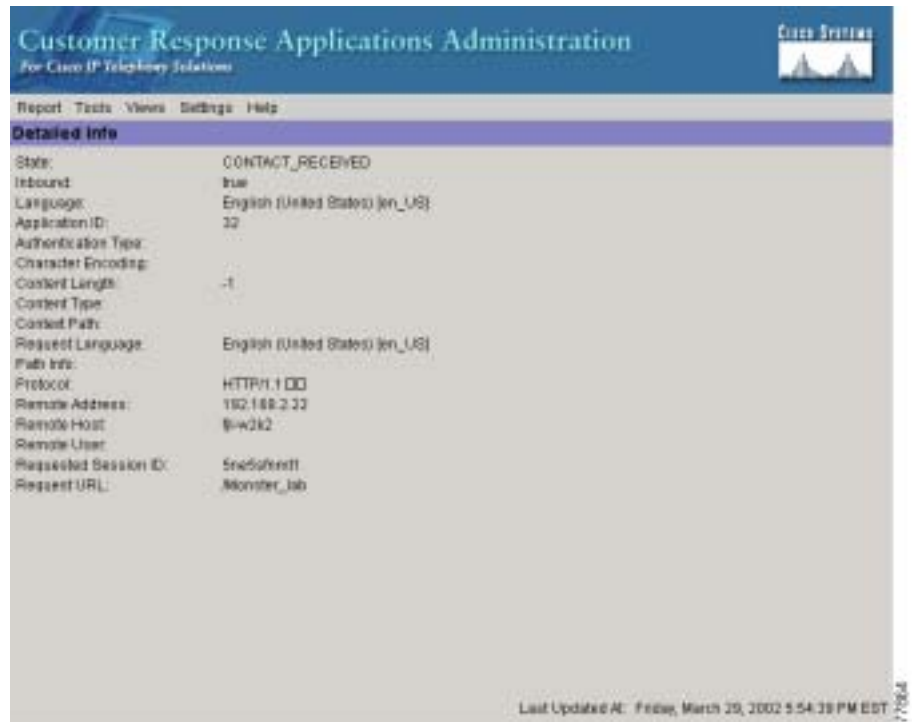
Row Heading	Description
State	Current state of the contact.
Inbound	If True, this e-mail message was received by the CRA server; if False, this e-mail was created by an application. **Note** Inbound e-mails are not currently supported.
Language	Selected language context of the e-mail message.
Application ID	ID of the associated application.
From	Sender of this e-mail message.
To	All the recipients of this e-mail message.
Subject	"Subject" field of this e-mail message.
Attachments	List of all attachments (file names) associated with this e-mail message.

Accessing Detailed HTTP Contact Information

Right-click a specific HTTP contact record in the Contacts web page to access the HTTP Detailed Info web page, which displays information for that specific record. (See Figure 18-11.)

Use the HTTP Detailed Info web page to view all information related to the HTTP contact.

Figure 18-11 HTTP Detailed Info Web Page

Table 18-10 describes the information provided on the HTTP Detailed Info web page.

Table 18-10 HTTP Detailed Info Web Page Rows

Row Heading	Description
State	Current state of the contact.
Inbound	If True, this HTTP request was received by the CRA server; if False, this HTTP request was created by an application. **Note** This information will always be reported as True, because the CRA server does not currently track outbound HTTP requests in this way.
Language	Language currently associated with the HTTP request.
Application ID	ID of the associated application.
Authentication Type	Name of the authentication scheme used to protect the servlet; for example, "BASIC" or "SSL."
Character Encoding	Length, in bytes, of the request body, which is made available by the input stream, or -1 if the length is not known. **Note** This length is the same as the value of the CGI[1] variable CONTENT_LENGTH.
Content Length	MIME type of the body of the request, or null if the type is not known. **Note** This is the same as the value of the CGI variable CONTENT_TYPE.
Content Type	Type of the Http contact request.
Request Language	Preferred language for client content (the language that the client accepts for its content), based on the Accept-Language header.
Path Info	Any extra path information associated with the URL the client sent when the HTTP request was made.

Table 18-10 HTTP Detailed Info Web Page Rows (continued)

Row Heading	Description
Protocol	Name and version of the protocol the request uses in the form: *protocol*/*majorVersion.minorVersion*; for example, HTTP/1.1 **Note** This value is the same as the value of the CGI variable SERVER_PROTOCOL.
Remote Address	IP address of the client that sent the request **Note** This value is the same as the value of the CGI variable REMOTE_ADDR.
Remote Host	Fully qualified name of the client that sent the request, or the IP address of the client, if the name cannot be determined **Note** This value is the same as the value of the CGI variable REMOTE_HOST.
Remote User	Login of the user making this request, if the user has been authenticated.
Requested Session ID	HTTP session ID as specified by the client.
Request URL	Section of the URL of the HTTP request, from the protocol name up to the query string in the first line of the HTTP request.

1. CGI = Common Gateway Interface

The Applications Menu Option

Choose **Reports > Applications** from the Application Reporting menu bar to access the Applications web page. (See Figure 18-12.)

Use the Applications web page to view all the applications loaded on the server.

Figure 18-12 Applications Web Page

Table 18-11 describes the information provided on the Applications web page.

Table 18-11 Applications Web Page Columns

Column Name	Description
Name	Unique name of the currently loaded application.
ID	Application ID.

Table 18-11 Applications Web Page Columns (continued)

Column Name	Description
Type	Type of application that is currently running (for example, a Cisco Script Application).
Description	Description of the application as entered on the CRA Administration web site.
Enabled	If True, the application is enabled; if False, the application is disabled.
Max. Sessions	Maximum number of simultaneous task instances that can run simultaneously on the CRA server.
Valid	If True, the application is valid; if False, the application is invalid.[1]

1. An application is valid if it was successfully loaded and initialized from its configuration. At any time, an application can become invalid if it internally fails to be refreshed.

The Sessions Menu Option

Choose **Reports > Sessions** from the Application Reporting menu bar to access the Sessions web page. (See Figure 18-13.)

Use the Sessions web page to view real-time information on all the active sessions.

Figure 18-13 Sessions Web Page

Table 18-12 describes the information provided on the Sessions web page.

Table 18-12 Sessions Web Page Columns
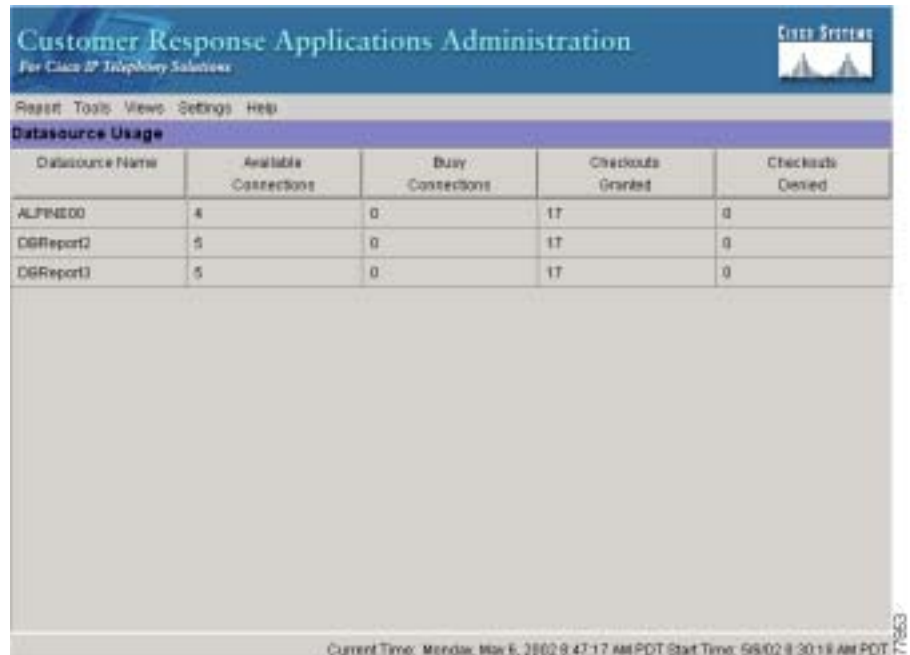
Column Name	Description
ID	Session ID. Note This identifier is guaranteed to remain unique for a period of 12 months. For more information, see the *Cisco Customer Response Applications Historical Reports User Guide*.
Mapping ID	User- or system-defined identifier that maps to this session.
Parent	Sessions that were created as a result of consult calls propagated in the system.
Creation Time	Creation time of the session.
State	Current state of the session. Note When marked IDLE, the session is subject to being "garbage collected" by the system after a specified period of time. In addition, a session is IN_USE if it still has a contact associated or a child session.
Idle Time	Length of time that the session has been idle.

The Datasource Usage Menu Option

Choose **Reports > Data source Usage** from the Application Reporting menu bar to access the Datasource Usage web page. (See Figure 18-14.)

Use the Datasource Usage web page to view real-time information on all configured datasource names (DSNs).

Figure 18-14 Datasource Usage Web Page

Table 18-13 describes the information provided on the Datasource Usage web page.

Table 18-13 Datasource Usage Web Page Columns

Column Name	Description
Datasource Name	Name of the datasource, as configured through the CRA Administration web interface.
Available Connections	Number of connections available.
Busy Connections	Number of busy connections. **Note** Busy + available = Maximum number of connections configured.
Checkouts Granted	Number of times the database connections have been used up since the statistics were last reset.
Checkouts Denied	Number of times the Database connections have been denied since the statistics were last reset.

The Overall IP ICD Stats Menu Option

Choose **Reports > Overall IP ICD Stats** from the Application Reporting menu bar to access the Overall IP ICD Stats web page. (See Figure 18-15.)

Use the Overall IP ICD Stats web page to view real-time ICD resource and call information.

Note   ICD reports contain information for ICD calls, which are calls that have been queued in one or more CSQs. If a call is not queued (for example, the caller hangs up before being queued), the reports do not display data for that call.

Figure 18-15 Overall IP ICD Stats Web Page

Table 18-14 describes the information provided on the Overall IP ICD Stats web page.

Table 18-14 Overall IP ICD Stats Web Page Rows

Row Heading	Description
CSQs	Number of CSQs currently configured. If a CSQ is added or removed, this statistic reflects that change.
Logged-in Resources	Number of resources currently logged in.
Talking Resources	Number of resources currently talking.
Ready Resources	Number of resources currently ready.
Not Ready Resources	Number of resources currently not ready.

Table 18-14 Overall IP ICD Stats Web Page Rows (continued)

Row Heading	Description
Total Contacts	Number of total ICD contacts that have arrived since the statistics were last reset. This includes contacts that are waiting, contacts connected to a resource, and contacts that have disconnected. If a resource transfers to or conferences with a route point, this value increases.
Contacts Waiting	Number of ICD contacts waiting to be connected to a resource. This column also displays how long the oldest contact in the queue has been waiting.
Contacts Handled	Number of ICD contacts that have been handled by a resource.
Contacts Abandoned	Number of ICD contacts that have arrived and disconnected before being connected to a resource.
Avg Talk Duration	Average duration that resources spend talking on ICD contacts. Talk duration starts when a contact first connects to a resource and ends when the contact disconnects from the last resource to which it was connected. Talk duration does not include hold time.
Avg Wait Duration	Average time contacts have waited to be connected to a resource. Wait begins when the contact is queued and ends when the contact stops waiting. Wait duration does not include hold time.
Longest Talk Duration	Longest talk duration of an ICD contact. Talk duration does not include hold time.
Longest Wait Duration	Longest wait for an ICD contact to be connected to a resource. Wait duration does not include hold time.

The CSQ IP ICD Stats Menu Option

Choose **Reports > CSQ IP ICD Stats** from the Application Reporting menu bar to access the CSQ IP ICD Stats web page. (See Figure 18-16.)

Note   ICD reports contain information for ICD calls, which are calls that have been queued in one or more CSQs. If a call is not queued (for example, the caller hangs up before being queued), the reports do not display data for that call.

Use the CSQ IP ICD Stats web page to view real-time ICD CSQ information.

Figure 18-16 CSQ IP ICD Stats Web Page

Table 18-15 describes the information provided on the CSQ IP ICD Stats web page.

Table 18-15 CSQ IP ICD Stats Web Page Columns

Column Name	Description
Name	Name of the CSQ.
Talking/ Ready Resources/ Not Ready Resources/ Logged-In Resources	Number of resources who are in the talking, ready, and not ready states, and the number of resources logged in for this CSQ. Values for the four items are separated by colons. Values are displayed in the same order that the items appear in the column heading.
Total Contacts	Number of total ICD contacts since the statistics were last reset for this CSQ.
Contacts Waiting	Number of ICD contacts waiting to be connected to a resource in this CSQ. This column also displays how long the oldest contact has been waiting.
Contacts Handled	Number of ICD contacts that have been handled by this CSQ.
Contacts Abandoned	Number of ICD contacts that have been abandoned by this CSQ.
Contacts Dequeued	Number of ICD contacts that have been dequeued from this CSQ.
Avg Talk Duration	Average time agents in this CSQ spend taking to ICD contacts .
Avg Wait Duration	Average time ICD contacts have waited to be connected to a resource in this CSQ. Wait begins when the contact is queued and ends when the contact stops waiting. Wait duration does not include hold time.

Table 18-15 CSQ IP ICD Stats Web Page Columns (continued)

Column Name	Description
Longest Talk Duration	Longest time agents in this CSQ spend talking to ICD contacts.
Longest Wait Duration	Longest wait for a contact to be connected to a resource.

The Resource IP ICD Stats Menu Option

Choose **Reports > Resource IP ICD Stats** from the Application Reporting menu bar to access the Resource IP ICD Stats web page. (See Figure 18-17.)

Use the Resource IP ICD Stats web page to view real-time ICD resource information.

Figure 18-17 Resource IP ICD Stats Web Page

Table 18-16 describes the information provided on the CSQ IP ICD Stats web page.

Table 18-16 Resource IP ICD Stats Web Page Columns

Column Name	Description
Name (ID)	Name (or ID) of the resource.
State	Current state of the resource.
Duration in State	Length of time the resource has remained in the current state.
Contacts Presented	Number of contacts that have been connected to this resource.
Contacts Handled	Number of contacts that have been handled by this resource.
Avg Talk Duration	Average time that this resource spends talking to ICD contacts.
Avg Hold Duration	Average time that the resource keeps ICD contacts on hold.
Longest Talk Duration	Longest time that this resource has spent talking to an ICD contact.
Longest Hold Duration	Longest time that this resource has placed an ICD call on hold.

The Tools Menu

The Tools menu gives you access to the following Application Reporting tools:

- **Reset All Stats**—Choose this option to reset all statistics.

- **Open Printable Report**—Choose this option to display a report that is optimized for printing.

This section contains the following topics:

The Reset All Stats Menu Option

Choose **Tools > Reset All Statistics** from the Application Reporting menu bar to reset all statistics. The CRA system resets all statistics.

Use the Reset All Stats option to reset all statistics accumulated since the last time the statistics were reset. It will not reset active statistics, such as active contacts, tasks, and so on.

Note   The CRA system automatically resets all statistics each day at midnight.

The Open Printable Report Menu Option

With a report open, choose **Tools > Open Printable Report** from the Application Reporting menu bar to create a printable version of that report. The CRA system opens a printable version of the report in a new browser window. (See Figure 18-18.)

Use the print functionality of your web browser to print the current report.

Figure 18-18 Printable Version of the Resource IP ICD Stats Web Page

The Views Menu

The Views menu allows you to access more detailed information for four reports: The Application Tasks report, the Contacts report, the Applications report, and the Sessions report.

> **Note**   For some reports, detailed information is also available by right-clicking a record in that report.

The Views menu contains different options, depending on the report you have chosen. Possible options are:

- **Contacts by Application Task ID**—Choose this option to view contacts according to Application Task ID numbers.
- **Engine Tasks by Application Task ID**—Choose this option to view Engine tasks according to Application Task ID numbers.
- **Detailed Info**—Choose this option to view more detailed information on selected reports.
- **Application Tasks by Application Name**—Choose this option to view application tasks by application name.
- **Contacts by Session ID**—Choose this option to view contacts by session ID.

This section contains the following topics:

Application Tasks

When you use the Views options with the Application Tasks reports, the Views menu contains the following options:

Contacts by Application Task ID

This report displays the same report as the Contact report (see the "The Contacts Menu Option" section on page 18-15,) with the exception that the Contacts by Application Task ID report has been filtered using only the contact currently being managed by the selected application task.

Engine Tasks by Application Task ID

This report displays the same report as the Engine Task reports (see the "The Engine Tasks Menu Option" section on page 18-13,) except that the Engine Tasks by Application Task ID report has been filtered to display only the engine tasks that are associated with the application task.

Contacts

When you use the Views options with the Application Tasks reports, the Views menu contains only the Detailed Info option.

The Detailed Info option provides various detailed information, depending on the type of contact selected. For example, if the contact is a call, the Calling Party number, the Called Number, and so on, are displayed for that particular call.

For more information, please see the "Accessing Detailed Call Contact Information" section on page 18-17.

Applications

When you use the Views options with the Application reports, the Views menu contains only the Application Tasks by Application Name option.

The Application Task By Application Name report displays the same report as the Application Task report (see Application Tasks, page 18-37), except that the Application Task By Application Name report is filtered using only the active application tasks associated with this application.

Sessions

When you use the Views options with the Session reports, the Views menu contains the following options:

- Contacts By Session ID, page 18-39
- Detailed Info, page 18-39

Contacts By Session ID

This report displays the same report as the Contact report (see the "The Contacts Menu Option" section on page 18-15,) with the exception that the Contacts By Session ID report is filtered using only the contacts associated with the selected session.

Detailed Info

Detailed info displays the time the session was created and its current state.

The Settings Menu

The Settings menu of the Application Reporting menu bar allows you to adjust various settings of the Real Time Reporting tool.

The Settings menu contains the following menu options:

- **Options**—Choose this option to set the polling (refresh) interval times and to set the amount of times the server will attempt to reconnect.
- **Window**—Choose this option to display reports in colors based on your Windows settings.
- **Motif**—Choose this option to display reports in purple and menu items in brown.
- **Metal**—Choose this option to display reports in grey and menu items in black.

This section contains the following topic:

- The Options Menu Option, page 18-40

The Options Menu Option

Choose **Settings > Options** to access the Options dialog box. Use the Options dialog box to set the polling (refresh) interval time, set the number of times the server will attempt to reconnect, and specify whether logged of agents appear in reports. Table 18-17 describes the fields in the Options dialog box.

Table 18-17 Options Dialog Box

Heading	Description
Polling Interval	Time between two requests to the server for new statistics by the client.
Server Connect Retry Count	The number of times that the CRA Administration web interface should attempt to reconnect to the CRA server.
	Note If an error occurs, an Error dialog box opens to alert you that the server is not communicating with the web interface.
Show Logged Off Resources	Specifies whether logged off agents appear in reports.

The Help Menu

The Help menu allows you to view system information and to access Cisco CRA online help.

The Help menu contains the following two options:

- **About**—Choose this option to display system information about the Real-time Reporting tool.

- **For This Page**—Choose this option to display online help files for that report.

This section contains the following topics:

About

Choose **Help > About** from the Application Reporting menu bar to display system information about the Real-time Reporting tool. The Application Reporting web page opens and displays the data host IP address and the data port number used by the Real-time Reporting tool. (See Figure 18-3.)

For This Page

From a specific report, choose **Help > For This Page** from the Application Reporting menu bar to display online help files for that report.

A separate browser window opens, displaying the section of the online help files that refers to the specific report.

The Real-time Snapshot Config Menu Option

Many call centers use wallboards to display their real-time reporting status. Wallboards can display data such as available agents in CSQs, call volumes, talk times, wait times, and number of handled calls. You can enable the CRA system to write ICD real-time information to a database that can then be displayed on a wallboard.

> **Note** You must purchase the wallboard separately, and configure and control it with its own wallboard software. Wallboard software and hardware are supported by the third-party wallboard vendors, not by Cisco.

You must install the wallboard software on a separate machine or desktop, not on the CRA server. During installation of your wallboard software, you will need to configure your wallboard software to access the CRA database. To do this, you need to assign a DSN, User ID, and password.

Choose **Tools > Real Time Snapshot Config** from the CRA Administration menu bar to access the Real-time Snapshot Writing Configuration for Wallboard web page. (See Figure 18-19.)

Use the Real-time Snapshot Writing Configuration for Wallboard web page to enable the system to write data to the wallboard system.

Cisco Customer Response Applications Administrator Guide

Figure 18-19 Real-time Snapshot Writing Configuration for Wallboard Web Page

Table 18-18 describes the fields in the Real-time Snapshot Writing Configuration for Wallboard web page.

Table 18-18 Real-time Snapshot Configuration Fields

Field	Description
Data Writing Enabled	If checked, the system writes the data to the database. If not checked, the system does not write the data to the database. The default is disabled.
Data Writing Interval	Sets the refresh interval for the wallboard data. Valid options: 5, 10, 15, 20, and 25.
ICD CSQs Summary	If checked, writes information about each CSQ to the RtCSQsSummary table in the CRA database. (See Table 18-19.)
ICD System Summary	If checked, writes overall ICD system summary to the RtICDStatistics table in the CRA database. (See Table 18-20.)

Table 18-19 describes the information written to the RtCSQsSummary database table.

Table 18-19 RtCSQsSummary Table Fields

Field	Description
CSQName	Name of the contact service queue.
loggedInAgents	Number of logged-in agents.
talkingAgents	Number of agents in talking state.
workingAgents	Number of agents in work state.
reservedAgents	Number of agents in the reserved state.
callsDequeued	Number of calls dequeued.
availableAgents	Number of available (Idle) agents.
unavailableAgents	Number of unavailable agents.
totalCalls	Total number of calls.
callsWaiting	Number of calls waiting.
callsHandled	Number of calls handled.
callsAbandoned	Number of calls abandoned.
startDateTime	Data collection starting time.
endDateTime	Last time this table data was updated.
convAvgTalkDuration	Average talk Duration in HH:MM:SS format.
convAvgWaitDuration	Average wait Duration in HH:MM:SS format.
convLongestTalkDuration	Longest talk Duration in HH:MM:SS format.
convLongestWaitDuration	Longest wait Duration in HH:MM:SS format.
convOldestContact	Oldest call in the queue in HH:MM:SS format.

Table 18-20 describes the information written to the RtICDStatistics database table.

Table 18-20 RtICDStatistics Table Fields

Fields	Description
totalCSQs	Number of CSQs configured.
loggedInAgents	Number of logged-in agents.
talkingAgents	Number of agents in talking state.
workingAgents	Number of agents in work state.
reservedAgents	Number of agents in the reserved state.
availableAgents	Number of available (Idle) agents.
unavailableAgents	Number of unavailable agents.
totalCalls	Total number of calls.
callsWaiting	Number of calls waiting.
callsHandled	Number of calls handled.
callsAbandoned	Number of calls abandoned.
startDateTime	Data collection starting time.
endDateTime	Last time this table data was updated.
convAvgTalkDuration	Average talk Duration in HH:MM:SS format.
convAvgWaitDuration	Average wait Duration in HH:MM:SS format.
convLongestTalkDuration	Longest talk Duration in HH:MM:SS format.
convLongestWaitDuration	Longest wait Duration in HH:MM:SS format.
convOldestContact	Oldest call in the queue in HH:MM:SS format.

The wallboard software must be installed on a separate machine or desktop, not on the CRA server. During installation of your wallboard software, you will need to configure your wallboard software to access the CRA database.

To do this, you need to create a system DSN (Data Source Name) on your Windows 2000 Professional or Windows 2000 server by performing the following procedure.

Procedure

Step 1 Go to **Start> Programs > Administrative Tools > Data Sources (ODBC)**.

The OBDC Data Source Administrator window opens.

Step 2 Click the System DSN tab and click **Add**.

The Create New Data Source window opens.

Step 3 In the Create New Data Source window, choose a SQL Server driver and click **Finish**.

The first Create a New Data Source to SQL Server window opens.

Step 4 In the first Create a New Data Source to SQL Server window, perform the following tasks:

- In the Name field, specify a name for this DSN (for example, Wallboard.)
- In the Description field, enter a descriptive name.
- In the Which SQL Server field, enter the CRA server IP address or system name.

Step 5 Click **Finish**.

The second Create a New Data Source to SQL Server window opens.

Step 6 In the second Create a New Data Source to SQL Server window, perform the following tasks:

- Check the SQL server authentication button.
- Use *wallboardUser* as login ID and password.

Step 7 Click **Next**.

The third Create a New Data Source to SQL Server window opens.

Step 8 In the third Create a New Data Source to SQL Server window, change the default database to *db_cra* and click **Next**.

The fourth Create a New Data Source to SQL Server window opens.

Step 9   In the fourth Create a New Data Source to SQL Server window, click **Finish**.

The ODBC Microsoft SQL Server window opens.

Step 10   In the ODBC Microsoft SQL Server window, click **Test Data Source**.

If the phrase "Test completed successfully" is returned, then click **OK**.

If the test is unsuccessful, return to the configuration sequence and fix any errors.

The Historical Reporting Menu Option

The Cisco CRA Historical Reporting subsystem provides you with a way to set up and manage the purging of the Historical Reporting databases.

Choose **Tools > Historical Reporting** from the CRA Administration menu bar to configure users and set up purging parameters for the Historical Reporting subsystem. The Historical Reporting Configuration web page opens.

Use the areas of the Historical Reporting Configuration web page to perform a variety of tasks, including configuring users, installing client software, and purging your database.

Note   For additional information on Historical Reporting, refer to the *Cisco Customer Response Applications Historical Reports User Guide*.

The Historical Reporting Configuration navigation bar contains the following hyperlinks:

- **Database Configuration**—Click this hyperlink to specify the maximum number of client and scheduler connections to the database server. If you have installed the Historical Reports Database server, you also specify the IP address of the that server.

- **User Configuration**—Click this hyperlink to choose the user for which you want to configure the Historical Reports.

- **Purge Schedule**—Click this hyperlink to set the purge schedule.

- **Purge Notification**—Click this hyperlink to specify the e-mail addresses to which you want purge notification to be sent.

- **Purge Now**—Click this hyperlink to manually purge data.

- **Synchronize Data**—Click this hyperlink to enable and set the automatic data synchronization schedule and to manually synchronize data. Synchronizing data is necessary only if the Historical Reports Database server is installed.

- This section contains the following topics:

The Database Configuration Hyperlink

Click the **Database Configuration** hyperlink on the navigation bar of the Historical Reporting Configuration web page to open the Database Configuration area from any other area of the Historical Reporting Configuration web page.

(The Database Configuration area automatically opens in the Historical Reporting Configuration web page when you first choose the **Historical Reporting** menu option from the Tools menu.)

Use the Database Configuration area to specify the maximum number of client and scheduler connections that can access the database server and, if the Historical Reports Database server is installed, to specify the IP address of that server.

This page also indicates the status of the Historical Reports Database server.

Table 18-21 shows the fields in the Database Configuration area of the Historical Reporting Configuration web page.

Table 18-21 Database Configuration Field

Field	Description
Historical Report DB Server	The IP Address of the database server.
Maximum DB Connections for Report Clients Sessions	The maximum number of client and scheduler connections that can access the Historical Reports Database server.

The changes take effect the next time that the CRA server is restarted.

Table 18-22 describes the buttons in the User Configuration for User area.

Table 18-22 Database Configuration for User Buttons

Button	Description
Update	Allow you to update the configuration information.

Related Topics

- Configuring the Database Server, page 9-5

The User Configuration Hyperlink

Click the **User Configuration** hyperlink on the navigation bar of the Historical Reporting Configuration web page to return to the User Configuration area from any other area of the Historical Reporting Configuration web page.

Use the User Configuration area to choose the user for which you want to configure the purge information for the CRA Historical Reports system.

Table 18-23 shows the field in the User Configuration area of the Historical Reporting Configuration web page.

Table 18-23 User Configuration Field

Field	Description
Search	Enables you to search for a specific Cisco CallManager user. You can use the search feature to find a specific user if there are more than 75 users.
Select User	User for which you want to configure the Historical Reports. This list contains up to 75 Cisco CallManager user names.

When you choose a user and click the Next button, the User Configuration for User area opens.

Use the User Configuration for User area to select a reporting package for this user from the list of installed reporting packages.

Table 18-24 describes the fields in the User Configuration for User area.

Table 18-24 User Configuration for User Fields

Fields	Description
Installed Reporting Package	All installed reporting packages available for this CRA system.
Selected Reporting Package	All reporting packages that are selected for this user.

Table 18-25 describes the buttons in the User Configuration for User area.

Table 18-25 User Configuration for User Buttons

Button	Description
Arrow	Allows you to move a highlighted package from one list to the other, depending on the direction of the arrow.
Update	Allow you to update the configuration information.

Related topic

- Configuring Users for Historical Reporting, page 9-10

The Purge Schedule Hyperlink

Click the **Purge Schedule** hyperlink on the navigation bar of the Historical Reporting Configuration web page to access the Purge Schedule area opens.

Use the Purge Schedule area of the Historical Reports Configuration web page to control the daily purge schedule and specify how long records should persist before the system purges them.

Table 18-26 describes the fields in the Purge Schedule area of the Historical Reporting Configuration web page.

Table 18-26 Purge Schedule Fields

Fields and Buttons	Description
Daily Purge at	Time of day for the daily purge.
Purge Data Older than *N* Months	Number of months data can persist before being purged.

Table 18-27 describes the button in the Purge Schedule area of the Historical Reporting Configuration web page.

Table 18-27 Purge Schedule Button

Name	Description
Update	Allows you to update the configuration information.

Related Topic

- Configuring Automatic Purging, page 9-12

The Purge Notification Hyperlink

Click the **Purge Notification** hyperlink on the navigation bar of the Historical Reporting Configuration web page to configure purge notification information. The Purge Notification area opens.

Use the Purge Notification area of the Historical Reports Configuration web page to specify when and to whom purge notification should be sent.

Table 18-28 describes the fields in the Purge Notification area of the Historical Reporting Configuration web page.

Table 18-28 Purge Notification Fields

Fields	Description
Send Email Notifications To	Email address(es) where notification is sent.
Send Email Notification When Database Exceeds *N* % of *maximum DB size*.	Percentage of the maximum database size at which notification is sent.
Initiate Automatic Purge When Database Exceeds *N* % of *maximum DB size*.	Percentage of the maximum database size at which an automatic purge is initiated.
Auto Purge Data for the Oldest *N* Days	Age of data to be purged.

Table 18-29 describes the button in the Purge Notification area of the Historical Reporting Configuration web page.

Table 18-29 Purge Notification Button

Name	Description
Update	Allows you to update the configuration information.

Related Topic

• Configuring Purge Notification Parameters, page 9-14

The Purge Now Hyperlink

Click the **Purge Now** hyperlink on the navigation bar of the Historical Reporting Configuration web page to manually purge data. The Purge Now area opens.

Use the Purge Now area to manually purge data.

✎

Note   The Purge Now area automatically displays the percentage of 2048 MB that is currently being used.

Table 18-30 describes the field in the Purge Now area of the Historical Reporting Configuration web page.

Table 18-30 Purge Now Field

Fields	Description
Purge Data Older Than *N* Months	Age of the data to be purged.

Table 18-31 describes the button in the Purge Now area of the Historical Reporting Configuration web page.

Table 18-31 Purge Now Button

Name	Description
Purge Now	Allows you to purge the specified data.

Related Topic

• Purging Manually, page 9-16

The Synchronize Data Hyperlink

Click the **Synchronize Data** hyperlink on the navigation bar of the Historical Reporting Configuration web page to open the Synchronize Data area from any other area of the Historical Reporting Configuration web page.

Use the Synchronize area if the Historical Reports Database server is installed to enable automatic historical and ICD configuration data synchronization, set the schedule or automatic data synchronization, and manually synchronize data.

This area also displays the status of automatic historical and configuration data synchronization.

Table 18-32 shows the fields in the Synchronize Data area of the Historical Reporting Configuration web page.

Table 18-32 Synchronize Data Field

Field	Description
Enable Historical Data Synchronizer	Allows you to enable or disable automatic historical data synchronization.
Synchronize historical data from local to remote database at	Allows you to set the time at which to synchronize historical data.
Enable Configuration Data Synchronizer	Allows you to enable or disable automatic ICD configuration data synchronization.
Synchronize configuration data from local to remote database every	Allows you to set the number of minutes after which to synchronize configuration data.

Table 18-33 describes the buttons in the Synchronize Data area.

Table 18-33 Synchronize Data Buttons

Button	Description
Update	Allow you to update the configuration information.
Cancel	Allows you to cancel
Synchronize Now	Allows you to synchronize the data manually.

Related Topic

- Synchronizing Data on the Local and Historical Report Databases, page 9-6

The Prompt Management Menu Option

Cisco CRA applications can use a wide variety of pre-recorded prompts to provide information to contacts and to elicit responses from contacts. The CRA system stores prompts in the repository. Prompts are managed by the Prompt Management tool of the CRA Administration web interface.

Choose **Tools > Prompt Management** from the CRA Administration menu bar to display, modify, or delete existing prompts and to add new prompts. The Prompt Management web page opens.

Use the Prompt Management web page to upload user prompts, delete prompts, or modify existing prompts stored on the CRA server or a network drive.

Table 18-34 describes the fields in the Prompt Management web page.

Table 18-34 Prompt Management Fields

Heading	Description
Language Directory	Location of the displayed prompts.
Codec	The codec chosen during installation for this CRA server. The codec cannot be changed in the CRA Administration web interface; it can only be changed through the installation process.
Name	Name of the prompt.
Length	File length (in bytes).
Delete	Allows you to deletes the prompt from the user repository of prompts.
Upload	Allows you to uploads a new version of this prompt.

Table 18-35 describes the buttons in the Prompt Management web page.

Table 18-35 Prompt Management Buttons

Name	Description
Create Folder	Displays a dialog box that lets you create a new folder.
Rename Folder	Displays a dialog box that lets you rename an existing folder.
Delete Folder	Displays a dialog box that lets you delete an existing folder and its contents.

The Prompt Management web page contains the following hyperlinks:

- **Add a New Prompt**—Click this hyperlink to add a new prompt.
- **Delete**—Click the **Delete** icon next to delete the existing folder.
- **Upload**—Click the **Upload** icon to upload a new prompt.

This section contains the following topics:

The Add a New Prompt Hyperlink

Click the **Add a New Prompt** hyperlink to access the Prompt Upload dialog box opens.

Use the Prompt Upload dialog box to add new prompts to the repository.

Note   For information on recording new prompts, see Recording a Prompt, page 7-12.

Table 18-36 describes the fields in the Add a New Prompt dialog box.

Table 18-36 Prompt Upload Dialog Box Fields

Heading	Description
Source File Name	Name of the .wav file that is the source file of the prompt.
Destination File Name	Name of the prompt you are adding.

Delete Icons

Click the **Delete** icon next to the name of any prompt displayed on the Manage Prompts web page to delete that prompt from the repository. A dialog box asks you to confirm the deletion. When you click OK, the CRA system deletes the selected script.

Use the **Delete** icon to delete prompts that are no longer used. When you delete a prompt, you permanently remove it from the repository and make it unavailable to the CRA system.

Upload Icons

Click the **Upload** icon next to the name of any prompt displayed on the Manage Prompts web page to upload a new prompt.

The Spoken Name Upload Menu Option

When a caller requests to be transferred to a specific extension, CRA applications can play back a recording of the spoken name of the person to whom the caller has called. These spoken name recordings are stored as .wav files and managed by the Spoken Name Upload tool of the CRA Administration web interface.

Choose **Tools > Spoken Name Upload** from the CRA Administration menu bar to upload these .wav files to a predetermined directory. The Spoken Name Prompt Upload web page opens.

Use the Spoken name Prompt Upload web page to upload spoken name .wav files.

The Spoken Name Prompt Upload web page also contains the **Click Here for More Recording Information** hyperlink, which displays a text file in your browser with more information on recording spoken name prompts.

Table 18-37 describes the fields in the Spoken Name Prompt Upload web page.

Table 18-37 Spoken Name Prompt Upload Web Page Fields

Field Heading	Description
User Id	User ID of the user for which the spoken name is to be uploaded.
Codec	The codec chosen during installation for this CRA server. The codec cannot be changed in the CRA Administration web interface; it can only be changed through the installation process.
Spoken Name (.wav)	Location of the .wav file.

Related Topic

• Adding a Prompt, page 7-13

The User Maintenance Menu Option

The User Maintenance menu option allows you to assign access levels to CRA system administrators and supervisors. Choose **Tools > User Maintenance** from the CRA Administration menu bar to assign administrative privileges to administrators and supervisors. The User Maintenance web page opens.

When you configure a CRA supervisor, you are configuring users who can access the CRA Supervisor web pages. You are not creating a supervisor for IP ICD.

Note   Only Administrators can update the CRA system. You must select at least one Administrator, so that someone is available to perform updates.

Table 18-38 shows the fields of the User Maintenance web page.

Table 18-38 User Maintenance Options

List Box or Drop-Down Menu fields	Description
Search	Enables you to search for a specific Cisco CallManager user.
CRA Administrator/ Supervisor List Box	Stores the administrators and supervisors. **Note** The Supervisor option is included with ICD packages only.
CMUsers List Box	Lists all of the Cisco CallManager users who can be added as CRA supervisors or administrators. This list box contains a maximum of 75 user names. You can use the search feature to find a specific user if there are more than 75 users.
Group Drop-Down Menu	Adds a user as an administrator or as a supervisor.

The Troubleshooting Tips Menu Option

The CRA system provides the Troubleshooting Tips tool as a way for you to search the troubleshooting database for suggestions on how to solve problems that may arise in the performance of your CRA system.

Note   For more information, refer to the *Cisco Customer Response Applications Troubleshooting Guide*.

Choose **Tools > Troubleshooting Tips** from the CRA Administration menu bar to search the CRA troubleshooting database for possible solutions to problems. The Troubleshooting Tips web page opens. (See Figure 18-20.)

Figure 18-20 Troubleshooting Tips Web Page

The Troubleshooting Tips web page also contains the **Cisco IP Telephony Technical Tips Website** hyperlink, which links to the Cisco IP Telephony Technical Tips website.

Table 18-39 shows the fields in the Troubleshooting Tips web page.

Table 18-39 Troubleshooting Tips List Box and Drop-Down Arrow

List Box or Drop-Down Menu Fields	Description
Components	Restricts the search to a specific CRA component. **Note** Selecting ALL will result in all components being searched for the problem keywords.
Enter Problem Keyword(s)	Searches the troubleshooting database for specific keywords.

■ **The Troubleshooting Tips Menu Option**

The Help Menu

The Help Menu of the Cisco Customer Response Applications (CRA) Administration web interface provides access to online help for the Cisco CRA system.

Use the Help menu to access configuration procedures and descriptions of CRA components.

The Help menu contains the following menu options:

- **Contents and Index**—Choose this option to view the entire Cisco CRA Administrator Guide online help system and index.

- **For this page**—Choose this option to view context-sensitive help.

- **About**—Choose this option to view CRA version information.

This chapter includes the following sections:

The Contents and Index Menu Option

To view the entire Cisco CRA Administrator Guide online help system and index, choose **Help > Contents and Index** from the CRA Administration menu bar. The Cisco CRA Administrator Guide Online Help window opens.

When you click on any topic in the left pane, the section of the online help that corresponds to that topic appears in the right pane.

Table 19-1 describes the menu options in the Cisco CRA Administrator Guide Online Help window.

Table 19-1   Online Help Menu Options

Menu Option	Description
Home	Returns you to the beginning of the online help document.
Search	Opens a search window, in which you can search for specific words in the online help files.
Using Help	Opens a file explaining how to use the online help files.
Glossary	Opens a glossary of definitions for terms used in the Cisco CRA Administrator Guide.
View PDF	Opens a PDF[1] version of the Cisco CRA Administrator Guide.
Contents	Displays the contents of the CRA Administrator Guide online help files in the left pane of the online help window.
Index	Displays the index of the CRA Administrator Guide online help files in the left pane of the online help window.

1. PDF = Portable Document Format

The For This Page Menu Option

To access context-sensitive help, go to the section for which you want help and choose **Help > For This Page** from the CRA Administration menu bar.

Figure 19-1   Help Menu—For This Page Menu Option
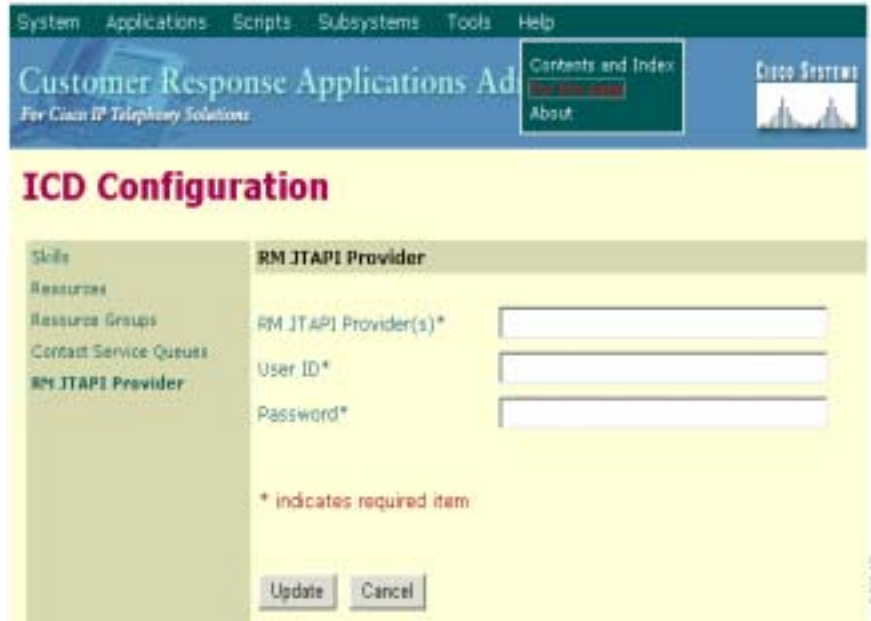
In this example, when you select **For This Page**, the section of the Cisco CRA Administration online help files that corresponds to the ICD Configuration web page opens.

The About Menu Option

To access CRA version information, choose **Help > About** from the CRA Administration menu bar. The CRA Application Administration web page opens.

To find out more detailed information, click the **Details** button. The Version web page appears, with information about installed files and their version number, date of installation, and size.

J

L

V